



8046-1041
PATENT

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant: Masayuki NAKAE et al. Confirmation No. Unknown
Appl. No.: 10/643,864 Group: Unknown
Filed: August 20, 2003 Examiner: Unassigned
For: ATTACK DEFENDING SYSTEM AND ATTACK
DEFENDING METHOD

L E T T E R

Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Date: December 1, 2003

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
Japan	2002-238989	August 20, 2002
Japan	2003-074781	March 19, 2003
Japan	2003-295020	August 19, 2003

Certified copies of the above-noted applications are attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

YOUNG & THOMPSON

By Benoît Castel

Benoît Castel, Reg. No. 35,041
745 South 23rd Street, Suite 200
Arlington, Virginia 22202
(703) 521-2297

Attachments

87 US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 8 月 2 0 日
Date of Application:

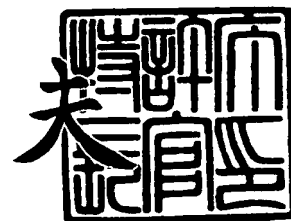
出 願 番 号 特 願 2 0 0 2 - 2 3 8 9 8 9
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 2 3 8 9 8 9]

出 願 人 日 本 電 気 株 式 有 限 公 司
Applicant(s):

2 0 0 3 年 8 月 2 0 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出 証 番 号 出 証 特 2 0 0 3 - 3 0 6 8 0 0 6

【書類名】 特許願
【整理番号】 35001159
【提出日】 平成14年 8月20日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 12/22
G06F 13/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 中江 政行

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 山形 昌也

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100097157

【弁理士】

【氏名又は名称】 桂木 雄二

【手数料の表示】

【予納台帳番号】 024431

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9303562

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 攻撃防御システムおよび攻撃防御方法

【特許請求の範囲】

【請求項 1】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、

前記おとり装置は、

前記ファイアウォール装置から転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、

前記ファイアウォール装置は、

入力 IP パケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力 IP パケットのヘッダ情報および振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記おとり装置へ転送した入力 IP パケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有することを特徴とする攻撃防御システム。

【請求項 2】 入力 IP パケットの前記ヘッダ情報は当該入力 IP パケットの送信元 IP アドレスおよび宛先 IP アドレスの少なくとも一方であり、

前記転送先選択手段は前記入力 IP パケットのヘッダ情報が前記振り分け条件を満たすか否かに依存して当該入力 IP パケットの転送先を決定する、

ことを特徴とする請求項 1 記載の攻撃防御システム。

【請求項 3】 前記転送先選択手段は、

前記内部ネットワークで使用されていない IP アドレスからなる誘導リストを前記振り分け条件として保持する格納手段を有し、

前記入力 IP パケットの宛先 IP アドレスと前記誘導リスト内の未使用 IP アドレスとが一致したときに当該入力 IP パケットを前記おとり装置へ転送する、

ことを特徴とする請求項 1 記載の攻撃防御システム。

【請求項 4】 前記ファイアウォール装置は、前記おとり装置へ転送した入力 I P パケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて、前記振り分け条件を更新する振り分け条件更新手段をさらに有することを特徴とする請求項 1 記載の攻撃防御システム。

【請求項 5】 前記フィルタリング条件管理手段は、前記おとり装置へ転送した入力 I P パケットのヘッダ情報に対応するフィルタリング条件を有効期限と共に設定し、前記入力 I P パケットに対応するフィルタリング条件の有効期限が超過している場合には、デフォルトのフィルタリング条件を前記パケットフィルタリング手段へ返すことを特徴とする請求項 1 記載の攻撃防御システム。

【請求項 6】 前記フィルタリング条件管理手段は、
前記攻撃検知手段が攻撃を検知した際の攻撃カテゴリと当該入力 I P パケットのアドレス情報とに対応したフィルタリング条件を生成する条件生成手段と、
前記条件生成手段により生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新するためのフィルタリング条件制御手段と、
を有することを特徴とする請求項 1 ないし 5 のいずれかに記載の攻撃防御システム。

【請求項 7】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、
前記ファイアウォール装置は、
入力 I P パケットのヘッダ情報および振り分け条件に基づいて、当該入力 I P パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力 I P パケットにおける各送信元 I P アドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記転送先選択手段は、前記入力 I P パケットの送信元 I P アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力 I P パケットの転送先を決定することを特徴とする攻撃防御システム。

【請求項 8】 前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度を更新することを特徴とする請求項 7 記載の攻撃防御システム。

【請求項 9】 前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度に所定数を加算することを特徴とする請求項 8 記載の攻撃防御システム。

【請求項 1 0】 前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度に対応する入力 I P パケットのパケットサイズが大きくなるほど値が小さくなる変数を、当該信頼度に加算することを特徴とする請求項 8 記載の攻撃防御システム。

【請求項 1 1】 前記信頼度管理手段は、前記入力 I P パケットが予め定められたプロトコルのパケットである場合のみ信頼度の更新を実行することを特徴とする請求項 8 記載の攻撃防御システム。

【請求項 1 2】 前記信頼度管理手段は、
複数の入力 I P パケットにおける各送信元 I P アドレスの信頼度と当該信頼度の最終更新時刻とを格納するための第 1 信頼度格納手段と、
前記第 1 信頼度格納手段の内容の複製を格納するための第 2 信頼度格納手段と、
前記信頼度格納手段に格納されたある信頼度が前記転送先選択手段によって取得されるごとに、当該信頼度を更新する第 1 更新処理手段と、
前記第 1 信頼度格納手段の内容を定期的に複製して前記第 2 信頼度格納手段へ格納するための複製処理手段と、
前記第 2 信頼度格納手段に格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を更新する第 2 更新処理手段と、
を有することを特徴とする請求項 7 記載の攻撃防御システム。

【請求項 1 3】 前記複製処理手段は、前記第 1 信頼度格納手段に格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を有するエントリを前記第 1 信頼度格納手段から削除することを特徴とする請求項 1 2 記載の攻撃防御システム。

【請求項 1 4】 前記第 2 更新処理手段は、前記最終更新時刻から所定期間

が経過した信頼度を所定値だけ低下させることを特徴とする請求項 12 記載の攻撃防御システム。

【請求項 15】 前記第 2 更新処理手段は、前記最終更新時刻から所定期間が経過した信頼度を前記第 2 更新処理手段から削除することを特徴とする請求項 12 記載の攻撃防御システム。

【請求項 16】 前記おとり装置は、前記ファイアウォール装置から転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有することを特徴とする請求項 7 記載の攻撃防御システム。

【請求項 17】 前記信頼度管理手段は、前記おとり装置へ転送した入力 IP パケットに関して前記攻撃検知手段が攻撃を検知したか否かに応じて、当該入力 IP パケットの送信元 IP アドレスの信頼度を更新することを特徴とする請求項 16 記載の攻撃防御システム。

【請求項 18】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、
前記ファイアウォール装置は、
第 1 転送先選択手段と、
第 2 転送先選択手段と、
複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を管理するための信頼度管理手段と、
を有し、

前記第 1 転送先選択手段は、入力 IP パケットのヘッダ情報および第 1 所定条件に基づいて、当該入力 IP パケットを前記第 2 転送先選択手段および前記おとり装置のいずれかへ転送し、

前記第 2 転送先選択手段は、前記第 1 転送先選択手段から転送された前記入力 IP パケットの送信元 IP アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が第 2 所定条件を満たすか否かに応じて当該入力 IP パケットの転送先を前記内部ネットワーク及び前記おとり装置のいずれかに決定する、
ことを特徴とする攻撃防御システム。

【請求項 1 9】 内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

IP パケットのフィルタリング条件および振り分け条件を用意し、

入力 IP パケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定し、

受理された入力 IP パケットのヘッダ情報および前記振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御方法。

【請求項 2 0】 入力 IP パケットの前記ヘッダ情報は当該入力 IP パケットの送信元 IP アドレスおよび宛先 IP アドレスの少なくとも一方であり、

前記入力 IP パケットのヘッダ情報が前記振り分け条件を満たすか否かに依存して当該入力 IP パケットの転送先を決定することを特徴とする請求項 1 9 記載の攻撃防御方法。

【請求項 2 1】 前記振り分け条件は、前記内部ネットワークで使用されていない IP アドレスからなる誘導リストであり、

前記入力 IP パケットの宛先 IP アドレスと前記誘導リスト内の未使用 IP アドレスとが一致したときに当該入力 IP パケットを前記おとり装置へ転送することを特徴とする請求項 1 9 記載の攻撃防御方法。

【請求項 2 2】 攻撃を検知したか否かに基づいて、前記振り分け条件を更新するステップをさらに有することを特徴とする請求項 1 9 記載の攻撃防御方法。

【請求項 2 3】 前記フィルタリング条件管理ステップは、

前記おとり装置へ転送した入力 IP パケットのヘッダ情報に対応するフィルタリング条件を有効期限と共に設定し、

前記入力 I P パケットに対応するフィルタリング条件の有効期限が超過している場合には、デフォルトのフィルタリング条件を設定する、

ことを特徴とする請求項 19 記載の攻撃防御方法。

【請求項 24】 前記フィルタリング条件管理ステップは、

攻撃を検知した際の攻撃カテゴリと当該入力 I P パケットのアドレス情報とに対応したフィルタリング条件を生成し、

生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新する、

ことを特徴とする請求項 19 記載の攻撃防御方法。

【請求項 25】 内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

I P パケットの振り分け条件を用意し、

複数の入力 I P パケットにおける各送信元 I P アドレスの信頼度を保持し、

入力 I P パケットの送信元 I P アドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力 I P パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とする攻撃防御方法。

【請求項 26】 前記信頼度を保持するステップは、

複数の入力 I P パケットにおける各送信元 I P アドレスの信頼度と当該信頼度の最終更新時刻とをリアルタイム信頼度データベースに格納し、

前記リアルタイム信頼度データベースに格納されたある信頼度がアクセスされるごとに当該信頼度を更新し、

前記リアルタイム信頼度データベースの内容を定期的に複製して長期信頼度データベースに格納し、

前記長期信頼度データベースに格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を更新する、

ステップを有することを特徴とする請求項 25 記載の攻撃防御方法。

【請求項 27】 前記おとり装置において、前記ファイアウォール装置から転送された入力 I P パケットに対するサービスプロセスを実行することで攻撃の

有無を検知するステップをさらに有することを特徴とする請求項 25 記載の攻撃防御方法。

【請求項 28】 攻撃が検知されたか否かに応じて、当該入力 IP パケットの送信元 IP アドレスの信頼度を更新するステップをさらに有することを特徴とする請求項 27 記載の攻撃防御方法。

【請求項 29】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力 IP パケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力 IP パケットのヘッダ情報および振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記おとり装置へ転送した入力 IP パケットに関して前記おとり装置が攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有することを特徴とするファイアウォール装置。

【請求項 30】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力 IP パケットのヘッダ情報および振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記転送先選択手段は、前記入力 IP パケットの送信元 IP アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力 IP パケットの転送先を決定することを特徴とするファイアウォール装置。

【請求項 31】 内部ネットワークと外部ネットワークとの境界に設置され

、おとり装置に接続されたファイアウォール装置において、

第1転送先選択手段と、

第2転送先選択手段と、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記第1転送先選択手段は、入力IPパケットのヘッダ情報および第1所定条件に基づいて、当該入力IPパケットを前記第2転送先選択手段および前記おとり装置のいずれかへ転送し、

前記第2転送先選択手段は、前記第1転送先選択手段から転送された前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が第2所定条件を満たすか否かに応じて当該入力IPパケットの転送先を前記内部ネットワーク及び前記おとり装置のいずれかに決定することを特徴とするファイアウォール装置。

【請求項32】 内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、

前記おとり装置へ転送した入力IPパケットに関して前記おとり装置が攻撃を検知したか否かに基づいて、当該入力IPパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有し、

前記転送先選択手段は、前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満た

すか否かに応じて当該入力 I P パケットの転送先を決定することを特徴とするファイアウォール装置。

【請求項 3 3】 前記おとり装置および前記ファイアウォール装置は単一ユニットに收容されていることを特徴とする請求項 1、7 および 1 8 のいずれかに記載の攻撃防御システム。

【請求項 3 4】 前記転送先選択手段は、
入力 I P パケットを格納するパケットバッファと、
前記入力 I P パケットを前記内部ネットワークに転送し、宛先到達不能メッセージを受信するか否かを監視する監視手段と、
を有し、

前記監視手段が宛先到達不能メッセージを受信した場合、対応する入力 I P パケットを前記パケットバッファから前記おとり装置へ転送することを特徴とする請求項 1 記載の攻撃防御システム。

【請求項 3 5】 コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御システムを実装するためのプログラムにおいて、

I P パケットのフィルタリング条件および振り分け条件を用意し、
入力 I P パケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力 I P パケットを受理するか否かを判定し、

受理された入力 I P パケットのヘッダ情報および前記振り分け条件に基づいて、当該入力 I P パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力 I P パケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力 I P パケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御プログラム。

【請求項 3 6】 コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御

システムを実装するためのプログラムにおいて、

IP パケットの振り分け条件を用意し、

複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を保持し、

入力 IP パケットの送信元 IP アドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とする攻撃防御プログラム。

【請求項 3 7】 コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたおとり装置を用いたファイアウォール装置を実装するためのプログラムにおいて、

IP パケットのフィルタリング条件および振り分け条件を用意し、

入力 IP パケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定し、

受理された入力 IP パケットのヘッダ情報および前記振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に対して、転送した入力 IP パケットに対するサービスプロセスを実行させることで攻撃の有無を検知させ、前記おとり装置が攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とするプログラム。

【請求項 3 8】 コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたおとり装置を用いたファイアウォール装置を実装するためのプログラムにおいて、

IP パケットの振り分け条件を用意し、

複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を保持し、

入力 IP パケットの送信元 IP アドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とするプログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明はコンピュータネットワークにおけるセキュリティ対策に係り、特に外部ネットワークからの攻撃に対して内部ネットワーク上の資源を保護するためのシステムおよび方法に関する。

【 0 0 0 2 】

【従来の技術】

従来、外部ネットワークからの攻撃に対する防御技術として、（１）ファイアウォール、（２）侵入検知システム、（３）おとりシステム、といった手法があった。

【 0 0 0 3 】

ファイアウォールの一例は、たとえば特開平 8 - 4 4 6 4 2 号公報に開示されている。外部の I P ネットワークと内部のイーサネット（登録商標）との境界にファイアウォールを設置し、検査対象となるパケットを外部ネットワークから内部ネットワークに通過させてよいか否かを判定する。特に、ファイアウォールにパケットフィルタを設け、パケットのヘッダ情報（送信元アドレスや送信先アドレス）などの他、プロトコルの種別（T C P / U D P / H T T P など）や、データ内容（ペイロード）なども参照しながら、所定のルールに従って、パケットの通過可否を判定する。適切なルールを設定しておけば、例えば、外部ネットワーク一般に公開されている W e b サーバなどに対してワームなどを含む不正なパケットが進入することを遮断できる。

【 0 0 0 4 】

侵入検知システムの一例は、たとえば特開 2 0 0 1 - 3 5 0 6 7 8 号公報に開示されている。この従来の侵入検知システムは不正侵入判定ルール実行部を有し、アプリケーションごとの判定ルール、例えば W W W サーバ用不正侵入判定ルールや M A I L サーバ用不正侵入判定ルールを備えている。まず、I P アドレステーブル取得部は、内部ネットワーク上を流れるパケットの送信元 I P アドレスも

しくは送信先 IP アドレスから、当該 IP アドレスを持つサーバにおいて現在動作中のアプリケーションを決定する。次に、不正侵入判定ルール実行部において、そのアプリケーションに応じた不正侵入判定ルールを実行し、当該パケットが不正であるか否かを判定する。こうすることにより、アプリケーションに依存したより精度の高い侵入検知が可能となる。

【0005】

おとりシステムの第1例は、たとえば特開 2000-261483 号公報に開示されている。この従来のおとりシステムは、ルータ 10 の下に構築された内部ネットワーク上に、トラフィック監視装置、攻撃パターンおよび偽装サーバを備える。まず、トラフィック監視装置において、内部ネットワーク上を流れるパケットを監視しながら、特定の攻撃パターンに合致するものを不正パケットとして検出し、その識別情報（送信元 IP アドレス、送信先 IP アドレスなどを含む）をルータに通知する。次に、ルータでは、後に続く外部ネットワークからのパケットについて、検出した識別情報に合致するパケットをすべて偽装サーバに転送する。偽装サーバは、転送されたパケットを適切に解釈し、内部ネットワーク上の正規のサーバをまねた偽の応答パケットを生成し、先に不正パケットを送信したホストへ向けて、その偽の応答パケットを送信する。こうすることで、外部ネットワーク上に存在する攻撃者に、内部ネットワークに悪影響のない形で、攻撃を続けさせることができ、逆探知によって攻撃者の身元を明らかにすることができる。

【0006】

おとりシステムの第2例は、たとえば特開 2002-7234 号公報に開示されている。この従来のおとりシステムは、内部ネットワークと外部ネットワーク（インターネット）との境界に、いわゆるゲートウェイとして、不正検出サーバと、おとりサーバと、を備える。外部ネットワークから内部ネットワークへ流れるパケットを不正検出サーバで監視し、例えば、当該パケットのペイロードについて所定のパターンマッチング処理を行うなどして、不正か否かを判定する。不正であると判定されたパケットには、その旨を示す特殊なマークを加えた上で、当該パケットをおとりサーバもしくは内部ネットワーク上の情報処理サーバへ転送

する。情報処理サーバへ不正パケットを転送する場合、予め情報処理サーバに不正回避処理部を持たせておき、特殊なマークのあるパケットを受信した際には、さらにおとりサーバへ当該パケットを転送するようにしておく。いずれにせよ、不正検出サーバで検出された不正パケットは、最終的におとりサーバへ到達する。その後、おとりサーバでは、偽の応答パケットを生成し、不正パケットの送信元ホストに向けて、当該応答パケットを送信する。こうすることで、不正と判定されたパケットは全ておとりサーバに閉じ込めることができる。

【0007】

さらに、おとりシステムの第3例は、たとえば特開平09-224053公報に記載されている。この従来のおとりシステムは、公衆ネットワーク（インターネット）と、プライベートネットワーク（内部ネットワーク）との境界に、スクリーン・システムおよび代行ネットワークを備える。スクリーン・システムは、自身に接続される各ネットワークからの着信パケットについて、パケットのヘッダに記載される情報や着信履歴など基にしたスクリーン基準に従い、フィルタリングを行う。ただし、スクリーン・システムの通信インタフェースはIPアドレスをもたず、tracerouteなどを用いた探索から自身を隠蔽することを特徴の1つとする。もう1つの特徴として、プライベートネットワークに向かう着信パケットについて、代行ネットワークに経路を変更することもできる。代行ネットワーク上には0台以上の代行ホストが設けられ、プライベートネットワーク上にあるホストの代理として動作させることもできる。こうすることで、公衆ネットワークからの攻撃からプライベートネットワークを保護できる。

【0008】

【発明が解決しようとする課題】

しかしながら、従来技術のいずれも、以下に挙げるような問題点を持つ。

【0009】

第1の問題点は、外部ネットワーク上の攻撃ホストと内部ネットワーク上のサーバとの間で、SSL（Secure Socket Layer）やIPSec（RFC2401記載）などの通信路暗号化技術が用いられた場合に、攻撃を有効に検知または防御できないということである。その理由は、攻撃検知のため

の主要なデータ（ペイロードなど）が暗号化されており参照できないためである。

【0010】

第2の問題点は、攻撃検知部のパフォーマンスが、近年のネットワークの高速化に追随しきれず、検査から漏れるパケットが存在したり、ネットワークの高速性を損なったりする点にある。その理由は、攻撃検知の精度を向上するには、より多彩な、あるいはより複雑な判定ルールの実行が必要であるが、一方、ネットワークの高速化により、検査対象となるパケット量が飛躍的に増加しているためである。

【0011】

また、上述した侵入検知システムやおとりシステムの第1例では、少なくとも1つの不正パケットが、内部ネットワーク上の保護すべきサーバに到達してしまう。その理由は、攻撃検知部が検査を行うのは、パケットのコピーでしかなく、当該パケットが不正と判定された場合でも、その内部ネットワーク上のパケット流通を遮断できないためである。

【0012】

さらに、上記おとりシステムの第3例では、インターネットから到来したパケットを代行ネットワークに経路変更させる条件および方法については検討されていない。このために、正確にパケットを振り分けることができず、正常なアクセスが代行ネットワークへ、異常なアクセスが内部ネットワークへ導かれる可能性がある。

【0013】

本発明の目的は、通信路暗号化技術を用いた通信システムに対しても、外部ネットワークからの攻撃を有効に防御できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

【0014】

本発明の他の目的は、高速ネットワーク環境に対応できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

【0015】

本発明のさらに他の目的は、保護すべきサーバに向けられた不正パケットを確実に遮断できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

【0016】

【課題を解決するための手段】

本発明の第1の観点によれば、おとり装置およびファイアウォール装置を含む攻撃防御システムが内部ネットワークと外部ネットワークとの境界に設置され、おとり装置はファイアウォール装置から転送された入力IPパケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、ファイアウォール装置は、入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて当該入力IPパケットを受理するか否かを判定するパケットフィルタリング手段と、受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、前記おとり装置へ転送した入力IPパケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて当該入力IPパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、を有する、ことを特徴とする。

【0017】

本発明の第2の観点によれば、ファイアウォール装置は、入力IPパケットのヘッダ情報および振り分け条件に基づいて当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、を有し、前記転送先選択手段は、前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特徴とする。

【0018】

本発明による攻撃防御方法は、入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力IPパケットの受理および廃棄のいずれかを実

行し、受理された入力 IP パケットのヘッダ情報および振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、前記入力 IP パケットが前記おとり装置へ転送されると、当該入力 IP パケットに対するサービスプロセスを実行し、前記サービスプロセスの実行状況を監視しながら、所定の攻撃カテゴリと関連づけられたルールに違反するか否かを判定することで攻撃の有無を検知し、前記入力 IP パケットに関して攻撃を検知したか否かに応じて、当該入力 IP パケットのヘッダ情報に対応するフィルタリング条件を設定し、入力した IP パケットのヘッダ情報に対応するフィルタリング条件に従ってパケットフィルタリングを実行する、ステップを有することを特徴とする。

【0019】

望ましくは、本発明によるファイアウォール装置は、入力 IP パケットのヘッダ情報およびフィルタリング条件に基づいて当該入力 IP パケットを受理するか否かを判定するパケットフィルタリング手段と、受理された入力 IP パケットのヘッダ情報および振り分け条件に基づいて当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を管理するための信頼度管理手段と、前記おとり装置へ転送した入力 IP パケットに関して前記おとり装置が攻撃を検知したか否かに基づいて当該入力 IP パケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、を有し、前記転送先選択手段は、前記入力 IP パケットの送信元 IP アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力 IP パケットの転送先を決定することを特徴とする。

【0020】

【発明の実施の形態】

(ネットワーク構成)

図1は、本発明による攻撃防御システムの概略的ブロック図である。本発明による攻撃防御システムは、基本的に、ファイアウォール装置1およびおとり装置2を有し、インターネット3と内部ネットワーク4との境界にファイアウォール

装置 1 が設置されている。内部ネットワーク 4 は、WWW (World-Wide Web) などのサービスを提供する 1 個以上のサーバ装置 401 を含む。ここではインターネット 3 に攻撃元ホスト 301 が想定されている。

【0021】

ファイアウォール装置 1 は、通常の正規のパケットであれば、これを通過させて内部ネットワーク 4 へ送付し、不正パケットあるいは不審なパケットであれば、おとり装置 2 へ誘導する。おとり装置 2 は攻撃の有無を検知し、攻撃を検知した場合にはアラートをファイアウォール装置 1 へ出力する。また、不正パケットに対する偽の応答パケットを生成してファイアウォール装置 1 へ返してもよい。ファイアウォール装置 1 はその偽の応答パケットを不正パケットの送信元である攻撃元ホスト 301 へ送信する。

【0022】

(第 1 実施形態)

1. 1) 構成

図 2 は、本発明の第 1 実施形態による攻撃防御システムのファイアウォール装置 1 およびおとり装置 2 の構成を示すブロック図である。ファイアウォール装置 1 は、外部通信インタフェース 100 でインターネット 3 と接続され、第 1 の内部通信インタフェース 104 で内部ネットワーク 4 と接続される。

【0023】

パケットフィルタ 101 は、外部通信インタフェース 100 および誘導部 103 の間に接続され、アクセス制御リスト管理部 102 から取得したアクセス制御ルールに従ってパケットフィルタリングを行う。後述するように、外部通信インタフェース 100 または誘導部 103 の一方から受け取った IP パケットを他方へ転送し、あるいは転送せずに廃棄する。

【0024】

パケットフィルタ 101 で受理されたパケットは誘導部 103 へ送られ、誘導部 103 は、後述する誘導リスト (図 5) を参照し、パケットフィルタ 101 から入力した IP パケットの宛先 IP アドレスに応じて当該パケットを第 1 の内部通信インタフェース 104 および第 2 の内部通信インタフェース 105 のいずれ

かへ誘導する。逆に、第1の内部通信インタフェース104または第2の内部通信インタフェース105からインターネット3に向かうIPパケットをパケットフィルタ101に転送する。

【0025】

第1の内部通信インタフェース104は、誘導部103から入力したIPパケットを内部ネットワーク4に伝達し、内部ネットワーク4からインターネット3に向かうIPパケットを誘導部103へ伝達する。第2の内部通信インタフェース105は、誘導部103によって誘導されたIPパケットをおとり装置2に伝達し、おとり装置2からインターネット3に向かうIPパケットを誘導部103に伝達する。

【0026】

おとり装置2は、プロセッサ201と攻撃検知部202とを含む。プロセッサ201は、WWWやTelnetなどのネットワークサービスを提供するプロセスを実行しながら、当該プロセスの状況を攻撃検知部202へ随時伝達する。攻撃検知部202は、プロセッサ201から入力されるプロセス状況を監視しながら、攻撃の有無を検査し、攻撃が認められた場合には攻撃内容を報告するためのアラートを生成しファイアウォール装置1へ送出する。

【0027】

制御インタフェース106を通してアラートを入力すると、防御ルール判定部107は、アラートの内容に従ってアクセス制御リスト管理部102のアクセス制御リストの更新等を指示する。

【0028】

図3は、図2のファイアウォール装置1におけるアクセス制御リスト管理部102の模式的構成図である。アクセス制御リスト管理部102は、アクセス制御リストデータベース1021、検索部1022および更新処理部1023を有する。アクセス制御リストデータベース1021は、少なくとも「ソースIPアドレス」、「ディスティネーションIPアドレス」および「フィルタ処理方法」といったフィールドを有するエントリ（アドレス制御ルール）の集合を検索可能に保持する。検索部1022は、パケットフィルタ101からIPアドレスなどを

含む問い合わせ (RQ) を受けると、アクセス制御リストデータベース 1021 から対応するアクセス制御ルールを検索してパケットフィルタ 101 へ返す。更新処理部 1023 は、防御ルール判定部 107 から入力した更新用アクセス制御ルールに従ってアクセス制御リストデータベース 1021 の内容を更新 (追加/修正) する。

【0029】

図4は、アクセス制御リストデータベース 1021 の内容を例示した模式図である。アクセス制御リストデータベース 1021 には複数のアクセス制御ルールが所定の規則に従って格納される。各アクセス制御ルールは、図4に示すように、ソースIPアドレス (SRC) やデスティネーションIPアドレス (DST) などのルール適合条件と、パケットの受理 (ACCEPT)、拒否 (DENY)、廃棄 (DROP) などの所定の処理方法 (PROC) を示す識別子との組からなる。アクセス制御ルールは一般に複数設定されるので、その集合をアクセス制御リストデータベース 1021 で保持しておく。図4において、アスタリスク (*) は任意のアドレスを示し、パケットフィルタ処理の “ACCEPT” はパケットの受理、“DENY” は ICMP エラー通知をするパケット拒否、“DROP” は ICMP エラー通知をしないパケット廃棄をそれぞれ示す。

【0030】

図5は、誘導部 103 に設けられた誘導リストの一例を示す模式図である。誘導部 103 には、予め1つ以上のIPアドレスからなる誘導リストが保持されている。本実施例の誘導リストでは、内部ネットワーク4の未使用IPアドレスが列挙されている。後述するように、未使用であるはずのIPアドレスを宛先とするパケットは、不審パケットである可能性が高い。

【0031】

図6は、防御ルール判定部 107 に保持されている防御ルールスクリプトを例示した模式図である。詳しくは後述するが、防御ルール判定部 107 は、探査 (RECON)、侵入 (INTRUSION)、破壊 (DESTRUCTION) などの攻撃種別ごとに、防御ルールを列挙し、例えばファイル形式で保持している。防御ルールは、所定の攻撃カテゴリに1対1対応する形式で、1つのアクセス制御ルールの雛型を指定する

記述が用いられる。例えば、

```
INTRUSION: (SRC:$ {SOURCE__IP__ADDRESS}  
, DST:*, PROC:DROP)
```

といった記述が行ごとに攻撃種別ごとに列挙されている。この記述のうち「\$ {SOURCE__IP__ADDRESS}」の部分が、後述するように、おとり装置 2 からのアラートに記載された情報（攻撃パケットのソース IP アドレス）で置き換えられる変数である。

【0032】

1. 2) 動作

1. 2. 1) パケットフィルタリング

図 7 は、本発明の第 1 実施形態による攻撃防御システムの動作を示すフローチャートである。まず、ファイアウォール装置 1 において、インターネット 3 から内部ネットワーク 4 へ向けた IP パケットを外部通信インタフェース 100 で捉えた後、当該 IP パケットをパケットフィルタ 101 へ転送する（ステップ A1）。

【0033】

次に、パケットフィルタ 101 は、当該 IP パケットのヘッダを参照し、そこに記載されているソース IP アドレスやディスティネーション IP アドレスなどの情報をアクセス制御リスト管理部 102 へ出力する。アクセス制御リスト管理部 102 は、上述したように、入力した IP アドレスを用いてアクセス制御リストデータベース 1021 を検索し、ヒットした最初のアクセス制御ルールをパケットフィルタ 101 へ返す。アクセス制御ルールを取得すると、パケットフィルタ 101 は、その処理方法に従って、当該 IP パケットを受理または廃棄する（ステップ A2）。IP パケットを受理した場合は、当該 IP パケットを誘導部 103 へ転送し、廃棄した場合は、直ちに次のパケットの処理へと制御を移す。

【0034】

アクセス制御リスト管理部 102 におけるアクセス制御ルールの検索において、パケットフィルタ 101 から入力したソース IP アドレスを検索部 1022 が受け取ると、検索部 1022 は個々のアクセス制御ルールの適合条件と入力した

ソース IP アドレスとを照合し、適合条件を満たす最初のアクセス制御ルールを抽出し、パケットフィルタ 101 へ返す。

【0035】

1. 2. 2) パケット誘導

次に、誘導部 103 では、パケットフィルタ 101 で受理された IP パケットに対して、そのデスティネーション IP アドレスと予め設けられた誘導リストとを参照し、転送すべき内部通信インタフェース (104 あるいは 105) を決定する (ステップ A3)。具体的には、図 5 に示すような誘導リストと、デスティネーション IP アドレスとを照合し、合致するものがある場合には、第 2 の内部通信インタフェース 105 を介して当該 IP パケットをおとり装置 2 へ転送する。合致するものがない場合には、第 1 の内部通信インタフェース 104 を介して内部ネットワーク 4 へ当該 IP パケットを伝達する。

【0036】

IP パケットが内部ネットワーク 4 へ伝達された場合には、当該 IP パケットは内部ネットワーク 4 上の適切なサーバ装置 301 に到達し、所定のサービスを提供するための処理が行われる (ステップ A4)。

【0037】

一方、IP パケットがおとり装置 2 へ伝達された場合には、そのプロセッサ 201 において、偽のサービスを提供するための処理を行いながら、入力データの内容や処理状況を逐次的に攻撃検知部 202 へ通知する (ステップ A5)。この際、おとり装置 2 は、ファイアウォール装置 1 から伝達された IP パケットを、そのデスティネーション IP アドレスの如何を問わず、受信することができる。具体的には、おとり装置 2 に複数の IP アドレスを割り当てられるような工夫を施してもよいし、あるいは図 8 に示すように、予め誘導部 103 にアドレス変換部 1031 を備えておき、入力 IP パケットのデスティネーション IP アドレスをおとり装置 2 の IP アドレスに書き換えた上で、おとり装置 2 に当該 IP パケットを伝達するような方法を用いてもよい。

【0038】

1. 2. 3) 偽サービス提供

IP パケットを受信後、おとり装置 2 は、偽のサービスとして、WWW や T e l n e t など 1 つ以上の任意のものを提供する。ただし、本実施形態においては、通信プロトコルさえ適切に処理すれば十分であり、実際のサービスで行われるような、ファイルシステムへのアクセスやデータベース処理などは一切行わなくともよい。具体的には、例えば、T e l n e t サービスの場合であれば、L o g i n / P a s s w o r d プロンプトへの任意の入力に対して、すべてログインを許可し、ユーザに偽のメッセージを応答するような偽装シェルを起動するようにしてもよい。

【0039】

1. 2. 4) 攻撃検知

次に、おとり装置 2 の攻撃検知部 202 では、プロセッサ 201 から通知される処理状況について、正常動作定義との照合を行い、攻撃の有無を判定する（ステップ A 6）。正常動作定義とは、おとり装置 2 上で提供されるサービスの正しい振舞いに関する条件の集合である。具体的には、例えば、WWW サービスに対して「WWW サービスに対応するプロセスは自ら他のサーバ装置にネットワークアクセスをすることはない」というような条件や、「/ u s r / l o c a l / w w w / l o g s ディレクトリ以外にファイルを書き込むことはない」というような条件などの集合である（詳しくは、図 12 参照）。これらの各条件と通知された処理状況とを照合し、合致しない条件を少なくとも 1 つ検出した際に、「攻撃あり」と判断する。

【0040】

攻撃を検出した際、違反した条件の意味に応じて、攻撃種別を決定し、その結果をアラートとしてファイアウォール装置 1 へ送信する（ステップ A 7）。

【0041】

攻撃種別とは、当該攻撃に対する防御方法を導出するに十分な分類をいい、例えば、

- ・「探査」：ポートスキャンやバナー攻撃などのいわゆる「フィンガープリンティング」
- ・「侵入」：トロイの木馬やアカウントの追加などのバックドア設置

・「破壊」：Ping Of Deathなどのサービス不能攻撃などを指す。その方法の一例として、正常動作定義の中の各条件について、違反時に想定される攻撃種別を予め併記しておけばよい。例えば、前記した「/usr/local/www/logsディレクトリ以外にファイルを書き込むことはない」という条件に違反するような攻撃については、バックドア設置の可能性が高いので、「侵入」を示す識別子を当該条件に併記しておく。

【0042】

1. 2. 5) アクセス制御リストの更新

最後に、ファイアウォール装置1における防御ルール判定部107では、制御インタフェース106を介しておとり装置2から受信したアラートを参照し、防御ルールを用いてアクセス制御ルールを生成し、アクセス制御リスト管理部102へ当該アクセス制御ルールを追加するよう指示する（ステップA8）。

【0043】

具体的には、防御ルール判定部107に、予め攻撃種別ごとに、図6のような防御ルールスクリプトを設定しておく。防御ルールスクリプトには、図6のような書式によって、攻撃種別と更新すべきアクセス制御ルールのひな型との組を記述する。アクセス制御ルールのひな型には、アラートに記載された情報を挿入するための変数が記述できる。たとえば、

(SRC:\$ {SOURCE_IP_ADDRESS}, DST:1. 2. 3. 4, PROC:DROP)

と記述されている場合、「\$ {SOURCE_IP_ADDRESS}」の箇所は、アラートに記載されたソースIPアドレスで置換され、

(SRC:12. 34. 56. 78, DST:1. 2. 3. 4, PROC:DROP)

といった完全な形式のアクセス制御ルールに変換される。そして、当該アクセス制御ルールは、アクセス制御リスト管理部102内の更新処理部1023へ伝達され、アクセス制御リストデータベース1021に適切に追加される。同じソースIPアドレスおよびデスティネーションIPアドレスの組をもつアクセス制御ルールが既にアクセス制御リストデータベース1021に登録されている場合

には、更新処理部 1023 は、新たに追加されたアクセス制御ルールが有効になるように適切にアクセス制御リストデータベース 1021 を更新する。たとえば、アクセス制御リストデータベース 1021 の検索スキャン方向の先頭に位置するように追加される。

【0044】

1. 3) 効果

第 1 実施形態のファイアウォール装置 1 では、誘導部 103 において、誘導リストとディスティネーション IP アドレスとの照合結果により、おとり装置 2 へ誘導する方法を用いている。このために、内部ネットワーク 4 の既存の構成を一切変更することなく、おとり装置 2 を設置可能となる。さらに、誘導リストに含める IP アドレスとして、内部ネットワーク 4 における未使用の IP アドレス群を記載することで、1 台のおとり装置 2 で、内部ネットワーク 4 上に複数のおとり装置 2 を設置するのと同じ効果が得られる。

【0045】

通常、「Code Red」や「Nimda」などの自動感染機能をもつワームは、ある連続した IP アドレスの区間からランダムに IP アドレスを選択しながら、感染を試みるよう動作する。したがって、おとり装置 2 は設置台数が多ければ多いほど検知の確率が高くなる。本実施形態では、図 5 に示すような誘導リストの作成でその効果を得ることができる。

【0046】

また、ファイアウォール装置 1 の外部通信インタフェース 100 に割り当てられた IP アドレスを誘導リストに含めることで、インターネット 3 側からは、ファイアウォール装置 1 とおとり装置 2 との見分けがつかなくなる。一般に、インターネット 3 からの攻撃は、ファイアウォールの発見から始まるので、本実施形態はファイアウォール装置 1 を「隠す」という効果をもつ。

【0047】

1. 4) 具体例

図 9～図 11 は第 1 実施形態の具体的動作例を説明するためのネットワーク構成図であり、図 12 はおとり装置 2 における攻撃検知動作を説明するための模式

図である。

【0048】

図9に示すように、インターネット3上に攻撃元ホスト301（IPアドレス：12.34.56.78）があり、内部ネットワーク4上にインターネットサーバ装置401がありものとする。さらに、インターネット3と内部ネットワーク4との境界にファイアウォール装置1が設置され、標準的なポート番号であるTCP80番ポートにおいてWWWサービスを提供するおとり装置2が設置されているものとする。また、内部ネットワーク4のネットワークアドレスとして、「1.2.3.x/24」が用いられており、サーバ装置401には「1.2.3.4」というIPアドレスが設定されているものとする。

【0049】

今、攻撃元ホスト301はWWWサービスに対する自動感染機能をもつワームに感染しており、当該ワームが次の感染先として、内部ネットワーク4に対応する「1.2.3.x/24」に狙いを定め、かつ「1.2.3.1」を第1の感染先として選択したものとする。このとき、攻撃元ホスト301から内部ネットワーク4に向けて、SYNパケット（ソースIPアドレス：12.34.56.78、ディスティネーションIPアドレス：1.2.3.1）が送信される。

【0050】

当該SYNパケットは、まず、ファイアウォール装置1の外部通信インタフェース100に到達した後、ただちにパケットフィルタ101に伝達される。パケットフィルタ101では、アクセス制御リスト管理部102に対して、少なくとも当該SYNパケットのソースIPアドレス「12.34.56.78」とディスティネーションIPアドレス「1.2.3.1」とを出力する。この他、アクセス制御ルールの粒度を高めるために、プロトコル番号「6」（TCPを示す）や、ポート番号「80」などを出力できるようにしてもよいが、本実施例では例としてソースIPアドレスとディスティネーションIPアドレスだけを入力するものとする。

【0051】

アクセス制御リスト管理部102におけるアクセス制御リストデータベース1

021は、例えば、図4のようなテキスト形式で記述されたアクセス制御リストを保持しているものとする。上述したように、各行は1つのアクセス制御ルールを示しており、SRCフィールドとDSTフィールドとの組が適合条件を、PROCフィールドがフィルタ処理方法をそれぞれ示す。

【0052】

検索部1022では、パケットフィルタ101から入力として与えられたソースIPアドレス「12.34.56.78」およびディスティネーションIPアドレス「1.2.3.1」との組を検索キーとして、適切なアクセス制御ルールを抽出するために、アクセス制御リストデータベースの先頭行から順に各アクセス制御ルールを参照しながら、各ルールの適合条件と前記入力との比較を行い、適合する最初のアクセス制御ルールを抽出する。この時点では、「(SRC：*，DST：1.2.3.1，PROC：ACCEPT)」(「PROC：ACCEPT」は入力IPパケットの受理を示す)というアクセス制御ルールが適合したとする。このとき、検索部1022は、「(SRC：12.34.56.78，DST：1.2.3.1，PROC：ACCEPT)」をパケットフィルタ101に返す。

【0053】

アクセス制御ルールを受け取ったパケットフィルタ101は、当該ルールのPROCフィールドを参照し、「ACCEPT」であることを確認すると、ただちに入力IPパケットを後段の誘導部103へと伝達する。

【0054】

続いて、誘導部103では、受け取った入力IPパケットのディスティネーションIPアドレスと内部的に保持する誘導リストとを参照し、次の転送先を決定する。本実施例では、誘導リスト内に内部ネットワーク4の未使用IPアドレスが列挙されており、その1つが「1.2.3.1」であるものとする。この場合、誘導部103は、入力IPパケットのディスティネーションIPアドレス「1.2.3.1」が誘導リストに記載されているのを確認した後、当該入力IPパケットをおとり装置2が接続されている第2の内部通信インタフェース105へと伝達する(図10参照)。

おとり装置 2 は、第 2 の内部通信インタフェース 105 へ伝達された全ての I P パケットを、そのディスティネーション I P アドレスの如何によらず受け付ける。おとり装置 2 では偽の W W W サービスが稼動しており、ワームが発した S Y N パケットを受け付けると共に、S Y N - A C K パケットをそのソース I P アドレス（すなわち攻撃元ホスト 301）へ向けて出力する。

これ以降、ファイアウォール装置 1 で同様の処理が繰り返されて、攻撃元ホスト 301 とおとり装置 2 との間で TCP 接続確立のための通信と、ワーム感染のための（不正な）通信が行われる。

おとり装置 2 では、プロセッサ 2 0 1 で WWW サービスを攻撃元ホスト 3 0 1 へ提供する。それと並行して、プロセッサ 2 0 1 は、ファイルアクセスやネットワークアクセスなどの動作状況を、攻撃検知部 2 0 2 へ逐次的に通知する。攻撃元ホスト 3 0 1 上のワームは、おとり装置 2 上の WWW サービスに対して、感染を試みる。具体的には、例えば、

「GET /default.ida?NNNNNNNNNNNNNNN(200
バイト程度の繰り返し) ...%u0000%u00=a HTTP/1.1」とい
った文字列から始まる、非常に大きなメッセージをWWWサービスに対して入力
し、いわゆる「バッファオーバーフロー」を引き起こすことで、任意のコマンド
を実行しようとする。この際、一般的なワームは、ワーム自身のコードをディス
ク上のシステム領域にコピーした後、当該コードを実行するようなコマンドを発
行する。したがって、ワームの侵入時に、プロセッサ201は、システム領域へ
ファイルの書き出しが行われたこと、あるいは、当該ファイルの実行が行われた
ことを攻撃検知部202に伝達することになる。このとき、同時に、おとり装置
2が受け付けた入力IPパケットのコピーも併せて伝達する。

攻撃検知部 202 は、予めプロセッサ 201 上の WWW サービスの適正な動作に関する情報を、正常動作定義ファイルとして保持している。正常動作定義ファ

イルは、例えば、図 12 のような形式で記述されており、ファイルの読み込み、書き出し、実行などに関する条件が列挙されている。

【0059】

ここで、前記ワームが自身のコピーを書き出す箇所を「C:¥Windows」ディレクトリだとすると、その動作は図 12 に示す正常動作定義ファイル内の第 2 番目の条件である

「WRITE, C:¥Inetpub¥wwwroot¥__vti__log¥* ; INTRUSION」(「C:¥Inetpub¥wwwroot¥__vti__log ディレクトリ以下にのみファイル書き出しを行う」の意)

に違反する。このとき、攻撃検知部 202 は、当該条件の「;」以下を参照し、INTRUSION (侵入) カテゴリに属する攻撃があったと判定する。

【0060】

続いて、攻撃検知部 202 は、少なくとも、入力 IP パケットに含まれるソース IP アドレスと、検出された攻撃のカテゴリが「INTRUSION」であることを知らせるためのアラートを生成し、ファイアウォール装置 1 の制御インタフェース 106 へ伝達する (図 11 参照)。

【0061】

制御インタフェース 106 で受信されたアラートは防御ルール判定部 107 へ伝達される。アラートの入力を受けた防御ルール判定部 107 は、上述したように、防御ルールを列挙したスクリプトを、例えばファイル形式で保持している。各防御ルールは、所定の各攻撃カテゴリに 1 対 1 対応する形式で、1 つのアクセス制御ルールのひな型が指定されている (図 6 参照)。

【0062】

具体的には、例えば、

INTRUSION: (SRC: \$ {SOURCE_IP_ADDRESS}
, DST: *, PROC: DROP) . . . (1)

といった記述が行ごとに列挙されている。ここで、アラートの入力を受けた防御ルール判定部 107 は、防御ルールの定義ファイルを行ごとに参照し、「INTRUSION」カテゴリに対応する防御ルールである式 (1) を抽出する。そし

て、アクセス制御ルールの雛型に対して、当該アラートに記載されたソース IP アドレス「12. 34. 56. 78」（すなわち攻撃元ホストの IP アドレス）によって、「\$ {SOURCE_IP_ADDRESS}」を置換し、

(SRC: 12. 34. 56. 78, DST: *, PROC: DROP)

... (2)

というアクセス制御ルールを生成する（「DST: *」は任意のディスティネーション IP アドレスに適合する）。そして、当該アクセス制御ルールをアクセス制御リスト管理部 102 へ伝達する。

【0063】

アクセス制御リスト管理部 102 では、防御ルール判定部 107 からのアクセス制御ルールの入力について更新処理部 1023 で処理する。更新処理部 1023 では、式 (2) で示されるアクセス制御ルールを、アクセス制御リストデータベース 1021 に伝達し、その追加を指示する。アクセス制御リストデータベース 1021 では、式 (2) で示されるアクセス制御ルールを追加するように更新処理を行う。その際、アクセス制御リストデータベース 1021 は、それ以降の検索処理が最近の更新結果を反映するように適切に更新処理を行う。例えば、図 4 のようなテキスト形式で記述されたアクセス制御リストを用い、先頭行から順に検索処理を行うような場合であれば、式 (2) を先頭行に追加すればよい。つまり、たとえ次式 (3) といったようなアクセス制御ルールが予め設定されていたとしても、

(SRC: 12. 34. 56. 78, DST: *, PROC: ACCEPT)

... (3)

当該更新処理以降、検索部 1022 がソース IP アドレス「12. 34. 56. 78」を含む入力を受けた場合には、式 (3) ではなく式 (2) を検索結果として出力する（図 13 参照）。

【0064】

次に、攻撃元ホスト 301 上のワームが次の攻撃先として、「1. 2. 3. 4」を選択したものとする。しかる後、先の攻撃と同様に、内部ネットワーク 4 上のサーバ装置 401 に向けた SYN パケットがファイアウォール装置 1 に到達す

る。その場合、当該SYNパケットの入力をうけたパケットフィルタ101は、アクセス制御リスト管理部102から適合するアクセス制御ルールとして式(2)を受け取るので、PROCフィールドの指定「DROP」に従い、当該SYNパケットを廃棄する(図14参照)。

【0065】

以上のような動作を行うことにより、本発明による攻撃防御システムは、攻撃元ホスト301上のワームからの攻撃から、内部ネットワーク4上のサーバ装置401を保護することができる。

【0066】

(第2実施形態)

2. 1) 構成

図15は、本発明の第2実施形態による攻撃防御システムのブロック図である。本実施形態のファイアウォール装置5は、図2に示す第1実施形態におけるファイアウォール装置1に信頼度管理部502を加え、さらに誘導部103に代えて、信頼度に依存してパケット誘導方向を決定できる誘導部501を有する。以下、図2に示すシステムと同じ機能ブロックについては、同一参照番号を付して詳細な説明は省略する。

【0067】

図15において、誘導部501は、パケットを入力すると、信頼度管理部502へ入力IPパケットのソースIPアドレスを出力し、対応する信頼度を取得する。信頼度を受け取ると、誘導部501はその信頼度と所定のしきい値との比較を行い、その結果に応じて、当該入力IPパケットを第1の内部通信インタフェース104および第2の内部通信インタフェース105のいずれかに出力する。

【0068】

信頼度管理部502はIPアドレスと対応する信頼度との組の集合を管理する。誘導部501から要求があると、信頼度管理部502はそれに対応した信頼度を検索して誘導部501へ返し、後述するように信頼度の更新を行う。

【0069】

2. 2) 動作

図16は、本発明の第2実施形態による攻撃防御システムの動作を示すフローチャートである。

【0070】

まず、第1実施形態のファイアウォール装置1と同様に、インターネット3からの入力IPパケットを受信すると（ステップA1）、パケットフィルタ101は、アクセス制御リスト管理部102で保持されているアクセス制御ルールの内容に応じて、当該入力IPパケットの受理または廃棄を行う（ステップA2）。受理されたIPパケットは誘導部501へ転送される。

【0071】

2. 2. 1) 信頼度管理

誘導部501は、入力IPパケットに含まれる情報のうち少なくともソースIPアドレスを信頼度管理部502へ出力し、当該IPアドレスに対する信頼度を取得する（ステップC1）。信頼度管理部502はIPアドレスとその信頼度との組の集合を保持し、IPアドレスを入力すると、それに対応する信頼度を出力することができる。具体的には、例えば、「1. 2. 3. 4 : 10」などのように、「<IPアドレス> : <信頼度>」といった形式をなす行で構成されるテキストファイルを用いることができる。

【0072】

その他、検索および更新処理を効率的に行うために、リレーショナルデータベースを利用してもよい。いずれにせよ、任意のIPアドレスについて、対応する信頼度を適切に検索および更新できればよい。信頼度管理部502は、入力されたIPアドレスに対応するIPアドレスと信頼度との組が1つ見つければ、当該信頼度を誘導部501へ出力する。もし適切なIPアドレスと信頼度の組が見つからなかった場合には、当該IPアドレスに対する信頼度として初期値（例えば0）を設定し、当該初期値を誘導部501に出力するとともに、新たに「<IPアドレス> : <初期値>」という組を保持内容に追加する。

【0073】

続いて、信頼度管理部502は、信頼度を出力した後、当該信頼度を増加させるように保持内容を更新する（ステップC2）。具体的には、例えば次式（4）

に示されるように、信頼度に定数 C (≥ 1) を加算する。

$$c[n+1] = c[n] + C \quad \dots \quad (4)。$$

【0074】

2. 2. 2) 信頼度に基づくパケット誘導

誘導部 501 は、取得した信頼度に応じて、当該 IP パケットの転送先を決定する（ステップ C3）。信頼度 c の評価処理の好適な一例としては、予め誘導部 501 にあるしきい値 T を設定しておき、信頼度 c としきい値 T との比較結果（大小関係）を評価する。

【0075】

図 17 は、本実施形態における信頼度とパケット転送先の関係を示すグラフである。ここでは、 $c \geq T$ のときには、入力 IP パケットを「信頼できる」と判定し、当該 IP パケットを内部通信インタフェース 104 を介して内部ネットワーク 4 へ伝達する。一方、 $c < T$ のときには、内部通信インタフェース 105 を介して、おとり装置 2 へ伝達する。

【0076】

なお、これ以降の動作は、図 7 に示す処理（ステップ A4～A8）と同じである。

【0077】

2. 2. 3) 信頼度の更新方法

図 16 のステップ C2 における信頼度の更新方法は、上述した式 (4) の他に、別の方法もある。次式 (5) に示すように、誘導部 501 からの入力の一部に、入力 IP パケット p のバイト数 $L(p)$ を含めておき、その逆数 $1/L(p)$ を加算するようにしても良い。

$$c[n+1] = c[n] + 1/L(p) \quad \dots \quad (5)。$$

【0078】

この方法は、大きなサイズをもつ IP パケットほど信頼度が増加しにくくなるように、重みづけを行うものである。一般に、バッファオーバーフロー攻撃やサービス妨害 (DoS) 攻撃を目的とした IP パケットは正常な通信内容をもつ IP パケットに比べて大きなサイズをもつことが多いため、こうした重みづけを施

すことで、これらの攻撃の可能性をもつ入力 IP パケットを、できるだけ長い期間、おとり装置 2 へ誘導することが可能になる。その結果、本発明による攻撃防御システムの防御性能を高めることができる。

【0079】

また、別の一例として、誘導部 501 からの入力の一部に、入力 IP パケットのプロトコル番号を含めておき、予め設定されたプロトコル番号に一致した場合のみ、信頼度を更新する方法を併用してもよい。たとえば、予めプロトコル番号「6」を設定しておくことで、入力 IP パケットが TCP である場合にのみ、信頼度を更新する。こうすることで、本格的な攻撃の前に準備的に行われるスキャン攻撃による、不要な信頼度の増加を抑える効果が得られる。もちろん、更新処理の条件として、プロトコル番号だけでなく、その他 IP ヘッダ、TCP ヘッダ、UDP ヘッダなどに含まれる任意の情報を用いてもよいし、複数の条件を組み合わせた論理式を用いるようにしてもよい。

【0080】

さらに別の一例として、入力 IP パケットについて、一般に外れ値検知として知られるような、統計的に「異常であること」の確からしさを求める方法を用いてもよい。具体的には、図 18 に示すように、IP アドレスと信頼度との組の集合に代えて、特開 2001-101154 公報（本出願人による特許出願）に記載の外れ値度計算装置を信頼度管理部 502 に組み込む。この場合、誘導部 501 からは実数値や属性を表す離散値などを含む多次元のベクトル、たとえば、 $x = (\text{入力 IP パケットの到達時刻}, \text{入力 IP パケットのサイズ}, \text{プロトコル番号})$ を入力する。

【0081】

このような多次元ベクトルを入力した外れ値度計算装置は、それまでの入力から生成した確率密度分布などを基に、1 個の実数値として表される「スコア値」を算出する。このスコア値は「異常であること」の確からしさを表しており、その値が大きいほど攻撃である可能性が高い、言い換えれば信頼度が低い。したがって、スコア値の逆数でもって、入力 IP パケットに対する信頼度とすることができる。

【0082】

図18 (A) は、外れ値度計算を用いた信頼度管理部502の概略的構成図であり、(B) は、その一例を示す詳細なブロック図である。この外れ値度計算を用いる方法は、上述したような「決定的な」信頼度の評価方法では捉えきれない（すなわち予期されない）攻撃を「確率的に」検出するものである。したがって、将来現れうる未知の攻撃に対する防御が可能となる。

【0083】

本発明の第2実施形態は、第1実施形態による効果に加えて、さらに「アクティブ・ターゲティング」にも対応できるという効果が得られる。アクティブ・ターゲティングとは、次に具体的に説明するように、予め特定のサーバ装置もしくはホスト装置に狙いを定めて行われる攻撃形態を指し、一般的には悪意をもった人間によって実行される。

【0084】

2. 3) 具体例

図19～図21は、本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【0085】

図19に示すように、インターネット3上の攻撃元ホスト301を使うユーザが、内部ネットワーク4上のサーバ装置401の動作停止を目的として、P i n g O f D e a t hなどのD o S攻撃を行う場合を考える。

【0086】

このような場合、攻撃元ホスト301のIPアドレス「12. 34. 56. 78」に対する信頼度が、誘導部501に設定されたしきい値以下であれば、図20に示すように、D o S攻撃を構成するIPパケットはおとり装置2へ誘導され、サーバ装置401は保護される。D o S攻撃をしかけるような悪意をもった人間は、ターゲットを定めたしばらく後に、攻撃を開始すると考えられるので、前記しきい値を十分大きく設定しておくことで、おとり装置2によるサーバ装置401の保護が達成される。

【0087】

さらに、通常の（すなわち攻撃の意図がない）ユーザからのアクセスについては、安全に内部ネットワーク 4 上のサーバ装置 401 によるサービスを行うができる。たとえば、図 21 に示すように、インターネット 3 上に通常のホスト 302 から、サーバ装置 401 へのアクセスがあった場合、前記例と同様に、ファイアウォール装置 5 の信頼度管理部 502 により、通常のホスト 302 の IP アドレスに対する信頼度が評価される。

【0088】

もし、通常のホスト 302 の信頼度が不十分であれば、誘導部 501 により「不審」と判定され、おとり装置 2 へ当該アクセスを構成する IP パケットは誘導される。ここで、おとり装置 2 のプロセッサ 201 で、サーバ装置 401 上の WWW サービスと同じ処理を行うよう、おとり装置 2 を設定しておく。すなわち、おとり装置 2 をサーバ装置 401 のミラーサーバとして動作させる。具体的には、WWW サービスの場合、HTML ファイルや JPEG ファイルなどのコンテンツの複製をとればよい。したがって、通常のホスト 302 は目的のサービスを受けることができる。おとり装置 2 では正常なアクセスがなされる間は攻撃が検知されないことなので、通常のホスト 302 の IP アドレスに対する信頼度は上述した信頼度更新方法に従って増加していき、いずれ、しきい値 T を超える。信頼度 c がしきい値 T を超えた後は、通常のホスト 302 からのアクセスを構成する IP パケットは内部ネットワーク 4 内のサーバ装置 401 へ誘導される。

【0089】

このような動作により、信頼ずみの通常のユーザからのアクセスについては、すべてサーバ装置 401 が応答する。したがって、おとり装置 2 が攻撃を受けて、その動作を停止したとしても、信頼ずみの通常のユーザは、サーバ装置 401 によりサービスを継続して受けることができるという効果をもつ。

【0090】

なお、おとり装置 2 はサーバ装置 401 上の完全なミラーサーバとして設定してもよいし、例えば、ユーザ認証を要するような重要サービスは除いて、一般的なサービスだけをおとり装置 2 で提供するようにも設定できる。

【0091】

(第3実施形態)

図22は、本発明の第3実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図であり、図23は、その一例を示す詳細なブロック図である。本実施形態のファイアウォール装置6は、ファイアウォール装置1における誘導部103に加えて、図5に示す第2実施形態の誘導部501および信頼度管理部502を有する。

【0092】

具体的には、図23に示すように、第1の誘導部103の後段として第2の誘導部501を設けても良い。逆に、第1の誘導部103の前段として第2の誘導部501を設けることもできる。

【0093】

いずれの構成においても、ワームのようにランダムにIPアドレスを選択して行われる攻撃と、アクティブ・ターゲッティングによる攻撃の両方に対応できる、という効果が得られる。また、あるホストが、第2の誘導部501で一旦信頼された後、ワームに感染するなどした場合でも、おとり装置2にて攻撃の有無を検査することができる、という効果も得られる。

【0094】

(第4実施形態)

4. 1) 構成

図24は、本発明における第4実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。本実施形態によるファイアウォール装置7は、図15のファイアウォール装置5における信頼度管理部502に代えて、信頼度管理部701が接続されている。その他の機能ブロックは、図15のものと同一であるから、同一参照番号を付して説明は省略する。

【0095】

図24に示すように、信頼度管理部701は、リアルタイム信頼度データベース7011、複製処理部7012、長期信頼度データベース7013、および、更新処理部7014を備える。

【0096】

リアルタイム信頼度データベース 7011 は、IP アドレス、それに対応する信頼度および最終更新時刻の組の集合を管理し、誘導部 501 からの問い合わせの IP アドレスに応じて、対応する信頼度を返す。複製処理部 7012 は、定期的に、リアルタイム信頼度データベース 7011 の内容を、長期信頼度データベース 7013 へ複製する。

【0097】

長期信頼度データベース 7013 は、IP アドレス、それに対応する信頼度および最終更新時刻の組の集合を管理する。更新処理部 7014 は、定期的に長期信頼度データベース 7013 を参照し、所定の期間よりも古い最終更新時刻を有する項目について、その信頼度を減算する更新処理を実行する。

【0098】

4. 2) 信頼度管理

基本的には、入力 IP パケットをフィルタリングし、おとり装置 2 または内部ネットワーク 3 へ誘導するまでの処理は、第 2 実施形態のファイアウォール装置 5 と同一である（図 16 のステップ A1～A2、C1～C3、A4～A8）。ただし、本実施形態の信頼度管理部 701 は、パケットの処理と並行して、以下にあげるような信頼度管理処理を行う。

【0099】

図 25 は信頼度管理部 701 における信頼度参照処理を示すフローチャートである。まず、図 16 のステップ C1 において信頼度の参照が行われたとき、信頼度管理部 701 は、リアルタイム信頼度データベース 7011 から、入力として与えられた IP アドレスに対応する項目が記録されているかどうかを調べる（図 25 のステップ D1）。当該 IP アドレスに対応する項目が記録されている場合（ステップ D1 の Y）、さらにその信頼度を参照し、当該信頼度を誘導部 501 に出力する（ステップ D2）。

【0100】

一方、IP アドレスに対応する項目がリアルタイム信頼度データベース 7011 に記録されていない場合（ステップ D1 の N）、まず、長期信頼度データベース 7013 を参照して、当該 IP アドレスに対応する項目が記録されているかど

うかを調べる（ステップD 3）。記録されている場合（ステップD 3のY）、長期信頼度データベース7 0 1 3の該当項目の内容（I Pアドレス、信頼度および最終更新時刻）を、リアルタイム信頼度データベース7 0 1 1にコピーし（ステップD 4）、信頼度を出力する（ステップD 2）。長期信頼度データベース7 0 1 3にも該当項目がない場合（ステップD 3のN）、リアルタイム信頼度データベース7 0 1 1に、所定の信頼度の初期値をもって、新たな項目を追加し（ステップD 5）、信頼度を出力する（ステップD 2）。

【0 1 0 1】

そして、図1 6のステップC 2において信頼度の更新が行われたとき、信頼度管理部7 0 1は、I Pアドレスと、信頼度の更新に加えて、更新時刻をリアルタイム信頼度データベース7 0 1 1に記録する。

【0 1 0 2】

4. 3) リアルタイム信頼度の複製処理

以上の処理に並行して、複製処理部7 0 1 2は定期的に（例えば1日ごとに）リアルタイム信頼度データベース7 0 1 1の全内容を走査しながら、各項目を長期信頼度データベース7 0 1 3へコピーしていく。このとき、最終更新時刻を参照して、所定の期間（例えば1週間）以上、更新処理が行われなかった項目について、当該項目をリアルタイム信頼度データベース7 0 1 1から削除する処理を行っても良い。

【0 1 0 3】

4. 4) 長期信頼度の更新処理

また、更新処理部7 0 1 4は、定期的に（例えば1日ごとに）長期信頼度データベース7 0 1 3の全内容を走査しながら、各項目の最終更新時刻を参照して、所定の期間（例えば1週間）以上、更新が行われなかった項目については、その信頼度を所定の値だけ減算する。もしくは、単に削除しても良い。

【0 1 0 4】

4. 5) 効果

以上のような動作を行うことで、リアルタイム信頼度データベース7 0 1 1の記憶容量を抑えることができるので、S D R A Mなど、低容量で高速な記憶デバ

イスを用いることができる。一方、長期信頼度データベース 7013 はアクセス頻度が少ないので、ハードディスクデバイスなど、大容量で低速な記憶デバイスを用いることができる。

【0105】

また、更新処理部 7014 による長期信頼度データベース 7013 の更新処理により、たとえ 1 度、十分な信頼度を得たソース IP アドレスについても、ある一定期間以上、アクセスが途絶えた場合には再び「不審」と見なすことができる。これは、特に中古 PC の売買など、ソース IP アドレスに相当するホストの利用環境が大きく変化した場合などに、信頼度の再評価を自動的におこなうことができるという効果をもつ。

【0106】

(第 5 実施形態)

本発明の第 5 実施形態として、図 23 に示す第 3 実施形態の信頼度管理部 502 に代えて、上述した第 4 実施形態の信頼度管理部 701 を用いたファイアウォール装置を構成することができる。基本的な構成は図 23 と同じであり、信頼度管理部 701 の構成及び動作は、図 24、図 25 および第 4 実施形態の項で説明した通りであるから、ここでは省略する。

【0107】

(第 6 実施形態)

6. 1) 構成

図 26 は、本発明の第 6 実施形態による攻撃防御システムのファイアウォール装置 9 を示す概略的ブロック図である。ファイアウォール装置 9 では、第 1 実施形態のファイアウォール装置 1 における誘導部 103 に代えて、バッファ 901 および ICMP 監視部 9012 を有する誘導部 901 が設けられている。本実施形態では、第 1 実施形態のように誘導リストを設けることなく、ICMP パケットを利用して同様の機能を実現できる。なお、簡略化のために、図 26 では他の機能ブロックの表示が省略されている。

【0108】

バッファ 9011 は、次に述べるように、パケットフィルタ 101 より受け取

ったパケットを一時的に蓄積し、第1内部通信インタフェース105を介して内部ネットワークへ転送すると共に、ICMP監視部9012からの求めに応じて、蓄積したパケットを第2の内部通信インタフェース105を介しておとり装置2へ再送信する。ICMP監視部9012は、第1の内部通信インタフェース104におけるICMPパケットの受信を監視し、特定のICMPエラーパケットを検出したとき、バッファ9011に適切なパケット再送を要求する。以下、本実施形態の動作を詳述する。

【0109】

6. 2) 動作

図27は本実施形態によるファイアウォール装置9の動作を示すフローチャートである。まず、第1実施形態のファイアウォール装置1と同様に、外部通信インタフェース100を介してインターネット4から受信した入力IPパケットについて、パケットフィルタ101によるフィルタリングを行う（ステップA1，A2）。

【0110】

受理されたIPパケットは誘導部901のバッファ9011に蓄積され（ステップE1）、無条件に第1の内部通信インタフェース104を介して内部ネットワーク3へ送出され（ステップE2）、通常のサービスが提供される（ステップA4）。この場合、たとえ不審パケットであっても内部ネットワークへ転送されてしまうが、実際の攻撃を実行する前に送信されるTCPコネクション確立要求のSYNパケットは攻撃要素が含まれていないために、SYNパケットであれば受け入れても問題はない。内部ネットワークにSYNパケットが転送され宛先が存在しなければ、到達不能を知らせるICMPパケット（タイプ3）が返される。

【0111】

ICMP監視部9012は、第1の内部通信インタフェース104でICMPパケット（RFC792記載）が受信されると、当該ICMPパケットの内容を参照して、到達不能を知らせるエラー（すなわちICMPタイプ3）であるか否かを調べる（ステップE3）。到達不能を知らせるエラーであれば（ステップE

3のY)、そのIPヘッダ部をさらに参照し、少なくともソースIPアドレスもしくはディスティネーションIPアドレスを用いてバッファ9011に再送要求を行う(ステップE3)。その他のメッセージであった場合は、何もせず、監視を続ける。

【0112】

再送要求を受けたバッファ9011は、少なくともソースIPアドレスもしくはディスティネーションIPアドレスに従って、蓄積されたパケットから該当するパケットを抽出し、当該パケットを第2の内部通信インタフェース105を介して、おとり装置2へ再送する(ステップE4)。以下、すでに述べたステップA5～A8が実行される。

【0113】

このように攻撃要素を含まないコネクション確立のためのパケットを利用することで、内部ネットワーク3の未使用IPアドレスを誘導リストとして事前に設定することなしに、自動的に未使用IPアドレス宛ての入力IPパケットをおとり装置2へ誘導することができる。

【0114】

(第7実施形態)

7. 1) 構成

図28は、本発明の第7実施形態による攻撃防御システムのファイアウォール装置10を示す概略的ブロック図である。このファイアウォール装置10は、上述した第2～第5実施形態によるファイアウォール装置における防御ルール判定部107およびアクセス制御リスト管理部102に代えて、有効期限付き防御ルール判定部1001および有効期限付きアクセス制御リスト管理部1002を設けている。

【0115】

防御ルール判定部1001は、制御インタフェース106を介しておとり装置2から受け取ったアラートに応じて、信頼度管理部502および701に対して、対応する信頼度の再設定を指示する。あるいは、アラートに応じて、更新すべきアクセス制御ルールを決定し、アクセス制御リスト管理部1002にその更新

を指示する。

【0116】

信頼度管理部502および701は、防御ルール判定部1001からの更新指示を受けて、新たな信頼度を決定し誘導部501へ出力する。アクセス制御リスト管理部1002は、防御ルール判定部1001からの更新指示を受けて、アクセス制御リストを更新し、パケットフィルタ101からの要求に応じてアクセス制御ルールを出力する。

【0117】

7. 2) 動作

本実施形態における攻撃防御システムの動作を、具体的な例を挙げながら詳細に説明する。

【0118】

まず、インターネット4から到達した入力IPパケットが、ファイアウォール装置10によって、おとり装置2へ誘導され、おとり装置2において、当該入力IPパケットによる攻撃が検知され、その旨を知らせるアラートが送信されるまでは、図16のステップA1～A7に示すように、第2～第5実施形態における攻撃防御システムと同様である。

【0119】

ファイアウォール装置10の防御ルール判定部1001には、防御ルール判定部107とは異なり、信頼度を更新するための防御ルールが予め設定されている。例えば、防御ルールとして、次式(6)のような形式の記述があれば、信頼度を1減算すると解釈されるものとする。

RECON: c (\$ {SOURCE__IP__ADDRESS}) -- = 1
... (6)。

【0120】

たとえば、制御インタフェース106を通してソースIPアドレス「12. 34. 56. 78」を示すアラートが受け取ると、防御ルール判定部1001はIPアドレス「12. 34. 56. 78」に対する信頼度を1減算すると解釈し、その旨を信頼度管理部502/701に指示する。すなわち、アラートを受け取

ると、そのソースIPアドレスの信頼度を低減させる。信頼度管理部502は第2実施形態で説明したように信頼度を更新し、信頼度管理部701は第4実施形態で説明したように信頼度を更新するから、信頼度の低減処理を加えることで、よりきめ細かい信頼度管理ができる。

【0121】

また、ファイアウォール装置10において、防御ルール判定部1001内に、防御ルール判定部107と同様に、アクセス制御ルールのひな型としての防御ルールを予め設定してもよい。ただし、この場合のアクセス制御ルールは、新たに「有効期間」を表すフィールドを記載できる（したがって防御ルールにも記載可能）。例えば、次式（7）に示すように、前記式（1）の防御ルールにEXPIREの項を追加し、「7日間有効」という制約をつけることができる。

```
INTRUSION: (SRC:$ {SOURCE__IP__ADDRESS} ,  
DST:*, PROC:DROP, EXPIRE:+7DAY) . . . (7)
```

。

【0122】

したがって、アラートが制御インタフェース106を経由して防御ルール判定部1001に伝達されると、防御ルール判定部107と同様の方法で、次式（8）に示すようにアクセス制御ルールが生成され、アクセス制御リスト管理部1002に伝達される。

```
(SRC:12.34.56.78, DST:*, PROC:DROP, EXPIRE:+7DAY) . . . (8)。
```

【0123】

次に、アクセス制御リスト管理部1002は、防御ルール判定部1001から受け取ったアクセス制御ルールをアクセス制御リストデータベース1021に追加する。このとき、式（8）のようにEXPIREフィールドがアクセス制御ルールに記載されている場合、アクセス制御リスト管理部1002は、現在時刻に、EXPIREフィールドに指定された値を加算した時刻を算出した上で、データベースを更新する（図7のステップA8に対応する）。

【0124】

図29は、アクセス制御リスト管理部1002の管理動作を示すフローチャートである。アクセス制御リストデータベース1021が更新された後、再びソースアドレス「12.34.56.78」からの入力IPパケットがファイアウォール装置10に到達すると、パケットフィルタ101は当該ソースIPアドレスをアクセス制御リスト管理部1002へ送付してアクセス制御ルールの取得要求を行う（ステップA2__1）。

【0125】

アクセス制御リスト管理部1002は、当該ソースIPアドレスに対応するアクセス制御ルールを検索する（ステップA2__2、A2__3）。式（8）に相当するアクセス制御ルールを抽出すると、アクセス制御リスト管理部1002は、EXPIREフィールドに記載された有効期間と現在時刻とを比較する（ステップA2__4）。

【0126】

現在時刻が有効期間を超過していた場合には（ステップA2__4のYES）、当該アクセス制御ルールをアクセス制御リストデータベース1021から削除し（ステップA2__5）、デフォルトのアクセス制御ルールをパケットフィルタ101へ返す（ステップA2__6）。逆に、有効期間内であれば（ステップA2__4のNO）、次式（9）に示すようなEXPIREフィールドを除いたアクセス制御ルールをパケットフィルタ101へ返す（ステップA2__7）。

(SRC:12.34.56.78, DST:*, PROC:DROP)

... (9)。

【0127】

こうして取得したアクセス制御ルールを用いて、パケットフィルタ101は受信IPパケットの受理／廃棄の判定を行う（ステップA2）。

【0128】

上述したように、攻撃をおとり装置で検知した後の防御方法として、よりきめ細かな対策を講じることができる。具体例を挙げると、一般に攻撃者は、「侵入」もしくは「破壊」に相当する攻撃の準備として、ポートスキャンあるいはTracerouteなどの「探査」に相当する攻撃を行う。しかし、「探査」とし

て検出されるアクセスが、全て攻撃であるとは限らないことも、よく知られる所である。したがって、「探査」に対する防御方法として、恒久的なアクセス遮断を行うことは不都合を生じる可能性がある。

【0129】

そこで、本実施形態では、有効期限付きのアクセス制御ルールを用いて時間制限を付けたアクセス遮断を行う。または、上述したように、アラーム発生によってそれまで蓄積された信頼度を低減させることで、信頼度がしきい値T（図17参照）を超えないようにし、おとり装置への誘導を継続し、後で「侵入」もしくは「破壊」に相当する攻撃を検知してから恒久的なアクセス遮断へと対応を変えることもできる。

【0130】

（第8実施形態）

図30は、本発明の第8実施形態による攻撃防御システムの概略的構成図である。第8実施形態では、単一のおとり装置2に代えて、2台以上のおとり装置2を含むおとりクラスタ21が設けられている。

【0131】

本実施形態における各おとり装置2は、特定のディスティネーションIPアドレスをもつパケット、もしくは、特定のポート番号をもつパケットにしか偽のサービスを提供しないようにする。

【0132】

こうすることにより、内部ネットワーク4上の特定のサーバ装置に1対1対応するおとり装置2を設けたり、特定の偽のサービスだけを提供するおとり装置2を設けたりすることができる。したがって、攻撃者に対して正規のサーバ装置により近いサービスを提供することができ、また、特定のサービス向けの正常動作定義をもつことでより運用性を向上させることもできる。

【0133】

（第9実施形態）

第9実施形態のファイアウォール装置は、第1～第8実施形態における誘導部に加えて、出力パケット誘導部を有する。出力パケット誘導部は、内部ネットワ

ーク 3 からインターネット 4 へ向けて送信される出力 IP パケットに対して、上述したパケットフィルタリングおよびおとり装置への誘導処理を行う。

【0134】

このような出力パケット誘導部を設けることで、内部ネットワーク 3 の運用規定として、インターネット 4 へのアクセスを禁じているような場合に、内部ネットワーク 3 からインターネット 4 への不法なアクセスを検知し、その記録をとることができる。

【0135】

(第 10 実施形態)

上記第 1 ～第 9 実施形態の説明では機能ブロック構成を用いたが、本発明はこれに限定されるものではなく、ソフトウェアにより同一の機能を実現することもできる。

【0136】

図 31 は、本発明の第 10 実施形態による攻撃防御システムの概略的構成図である。本実施形態のファイアウォール装置には、プログラム制御プロセッサ 1101、上記第 1 ～第 9 実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ 1102、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース 1103、および各種インタフェース 100、104 ～ 106 が設けられている。同様に、本実施形態のおとり装置には、プログラム制御プロセッサ 2101、上記第 1 実施形態で説明したおとり装置としての機能ブロックを実現するプログラムのセットを格納したプログラムメモリ 2102 およびファイアウォール装置とのインタフェースが設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第 1 ～第 9 実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。

【0137】

(第 11 実施形態)

上記第 1 ～第 10 実施形態では、ファイアウォール装置とおとり装置とが別ユニットになった攻撃防御システムを例示したが、本発明はこれに限定されるもの

ではなく、ハードウェア的に1ユニットで構成することもできる。1ユニットは、取り扱いが容易であり小型化し易いというメリットがある。

【0138】

図32は、本発明の第11実施形態による攻撃防御ユニットの概略的構成図である。本実施形態の攻撃防御ユニットには、ファイアウォール装置用のプログラム制御プロセッサ1101、おとり装置用のプログラム制御プロセッサ2101、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース1103、上記第1～第9実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ1104、および各種インタフェース100および104が設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第1～第9実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。また、プロセッサ1101とプロセッサ2101とを単一のプロセッサで構成しても良い。

【0139】

【発明の効果】

以上詳細に説明したように、本発明による攻撃防御システム及び方法によれば、IPパケットのヘッダ情報に基づいてパケットの誘導を行うために、外部ネットワークから内部ネットワークへのアクセスにおいて通信路暗号化技術が用いられた場合でも、攻撃を検知および防御することができる。いかなる通信路暗号化技術が用いられたとしても、少なくともIPヘッダに記載されたソースIPアドレスもしくはディスティネーションIPアドレスは暗号化されず、さらにファイアウォール装置によるおとり装置への誘導は、これらIPヘッダに記載された情報を基に行うことができるためである。

【0140】

また、本発明によれば、ファイアウォール装置によるおとり装置への誘導方法が少ないパラメータを基にした簡易なアルゴリズムで実現できるため、高速ネットワーク環境においても、ネットワーク性能を高いレベルで維持できる。

【0141】

さらに、本発明によれば、おとり装置へ誘導されて攻撃が検出された全てのパケットについて、その送信元ホストからの以降のアクセスを拒否するように動的な防御を行うことで後続する攻撃を全てファイアウォール装置で防御することができる。このために内部ネットワークへの通信経路が無くなり、検出された攻撃用パケットが一切内部ネットワークに到達しない。

【図面の簡単な説明】

【図 1】

本発明による攻撃防御システムの概略的ブロック図である。

【図 2】

本発明の第 1 実施形態による攻撃防御システムのファイアウォール装置 1 およびおとり装置 2 の構成を示すブロック図である。

【図 3】

図 2 のファイアウォール装置 1 におけるアクセス制御リスト管理部 102 の模式的構成図である。

【図 4】

アクセス制御リストデータベース 1021 の内容を例示した模式図である。

【図 5】

誘導部 103 に設けられた誘導リストの一例を示す模式図である。

【図 6】

防御ルール判定部 107 に保持されているアクセス制御ルールのひな型を例示した模式図である。

【図 7】

本発明の第 1 実施形態による攻撃防御システムの動作を示すフローチャートである。

【図 8】

本発明の第 1 実施形態のファイアウォール装置でアドレス変換処理を行う際の好適な一例を示すブロック図である。

【図 9】

第 1 実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図 1 0】

第 1 実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図 1 1】

第 1 実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図 1 2】

おとり装置 2 における攻撃検知動作を説明するための模式図である。

【図 1 3】

第 1 実施形態におけるアクセス制御リストの更新動作例を説明するための模式図である。

【図 1 4】

第 1 実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図 1 5】

本発明の第 2 実施形態による攻撃防御システムのブロック図である。

【図 1 6】

本発明の第 2 実施形態による攻撃防御システムの動作を示すフローチャートである。

【図 1 7】

本実施形態における信頼度とパケット転送先の関係を示すグラフである。

【図 1 8】

(A) は、外れ値度計算を用いた信頼度管理部 5 0 2 の概略的構成図であり、
(B) は、その一例を示す詳細なブロック図である。

【図 1 9】

本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図 2 0】

本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図 2 1】

本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワ

ーク構成図である。

【図 2 2】

本発明の第 3 実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図である。

【図 2 3】

第 3 実施形態による攻撃防御システムのファイアウォール装置の一例を示す詳細なブロック図である。

【図 2 4】

本発明における第 4 実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。

【図 2 5】

信頼度管理部 7 0 1 における信頼度参照処理を示すフローチャートである。

【図 2 6】

本発明の第 6 実施形態による攻撃防御システムのファイアウォール装置 9 を示す概略的ブロック図である。

【図 2 7】

本実施形態によるファイアウォール装置 9 の動作を示すフローチャートである。

【図 2 8】

本発明の第 7 実施形態による攻撃防御システムのファイアウォール装置 1 0 を示す概略的ブロック図である。

【図 2 9】

アクセス制御リスト管理部 1 0 0 2 の管理動作を示すフローチャートである。

【図 3 0】

本発明の第 8 実施形態による攻撃防御システムの概略的構成図である。

【図 3 1】

本発明の第 1 0 実施形態による攻撃防御システムの概略的構成図である。

【図 3 2】

本発明の第 1 1 実施形態による攻撃防御ユニットの概略的構成図である。

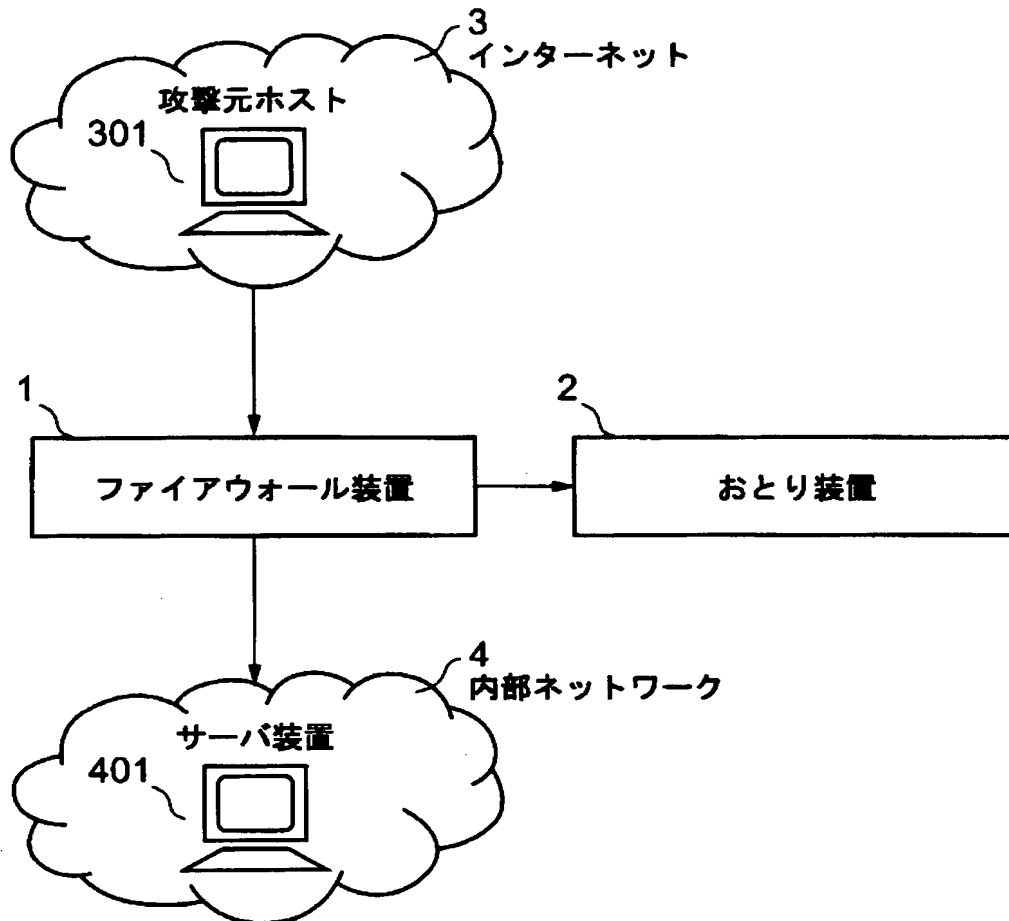
【符号の説明】

- 1 ファイアウォール装置
 - 1 0 0 外部通信インタフェース
 - 1 0 1 パケットフィルタ
 - 1 0 2 第 1 のアクセス制御リスト管理部
 - 1 0 2 1 アクセス制御リストデータベース
 - 1 0 2 2 検索処理部
 - 1 0 2 3 更新処理部
 - 1 0 3 誘導部
 - 1 0 3 1 アドレス変換部
 - 1 0 4 第 1 の内部通信インタフェース
 - 1 0 5 第 2 の内部通信インタフェース
 - 1 0 6 制御インタフェース
 - 1 0 7 防御ルール判定部
- 2 おとり装置
 - 2 0 1 プロセッサ
 - 2 0 2 攻撃検知部
- 3 インターネット
 - 3 0 1 攻撃元ホスト
 - 3 0 2 通常のホスト
- 4 内部ネットワーク
 - 4 0 1 サーバ装置
- 5 ファイアウォール装置
 - 5 0 1 誘導部
 - 5 0 2 信頼度管理部
 - 5 0 2 1 外れ値検知部
- 6 ファイアウォール装置
- 7 ファイアウォール装置
 - 7 0 1 信頼度管理部

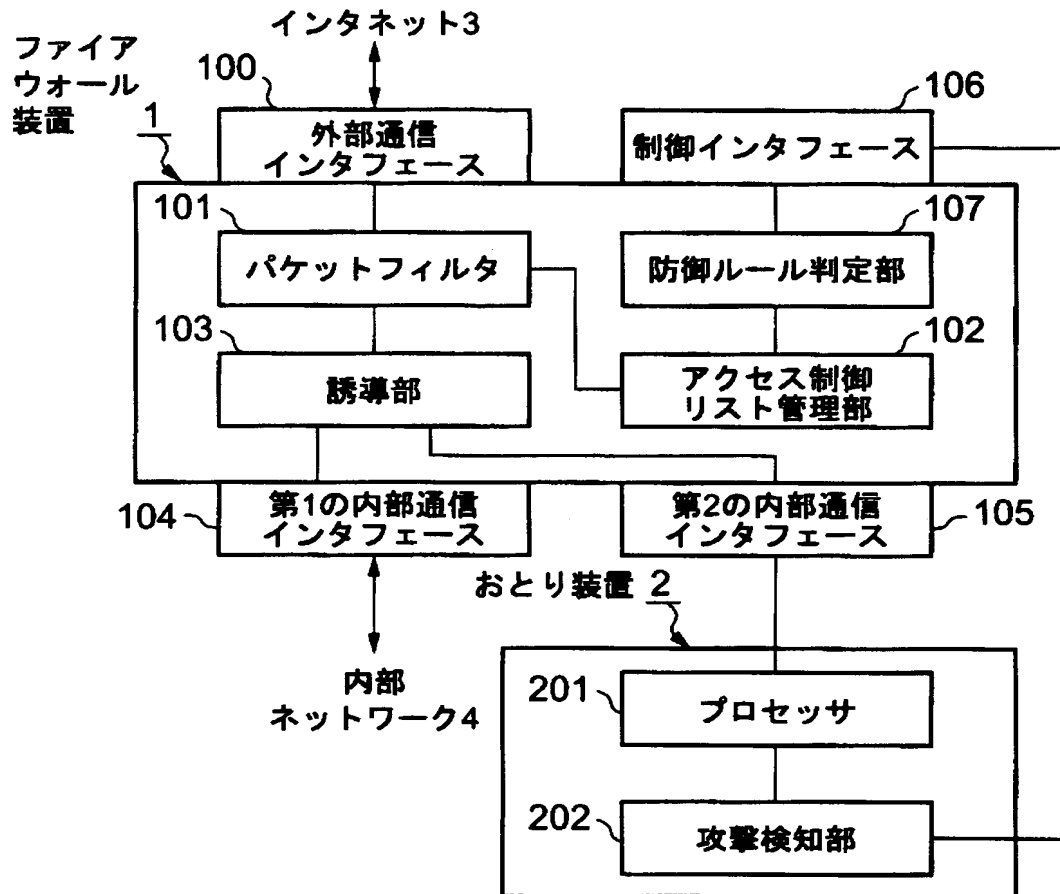
- 7 0 1 1 リアルタイム信頼度データベース
- 7 0 1 2 複製処理部
- 7 0 1 3 長期信頼度データベース
- 7 0 1 4 更新処理部
- 8 ファイアウォール装置
- 9 ファイアウォール装置
- 9 0 1 誘導部
- 9 0 1 1 バッファ
- 9 0 1 2 I C M P 監視部
- 1 0 ファイアウォール装置
- 1 0 0 1 防御ルール判定部
- 1 0 0 2 アクセス制御リスト管理部
- 2 1 おとりクラスタ

【書類名】 図面

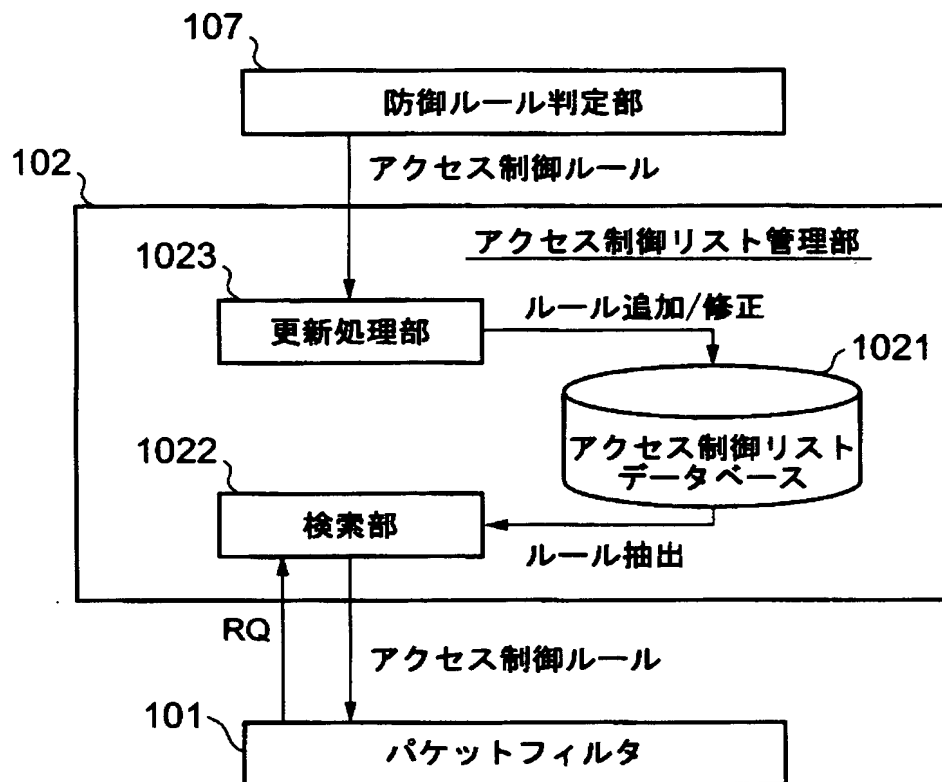
【図 1】



【図 2】



【図 3】



【図 4】

1021

アクセス制御リストデータベース		
ソースIPアドレス (SRC)	デスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

*…任意のアドレスにマッチ

ACCEPT…パケットの受理

DENY…パケットの拒否(ICMPエラーを通知)

DROP…パケットの廃棄(ICMPエラーを通知しない)

【図 5】

誘導リスト

1.2.3.1
1.2.3.2
1.2.3.3
1.2.3.5
1.2.3.6
⋮

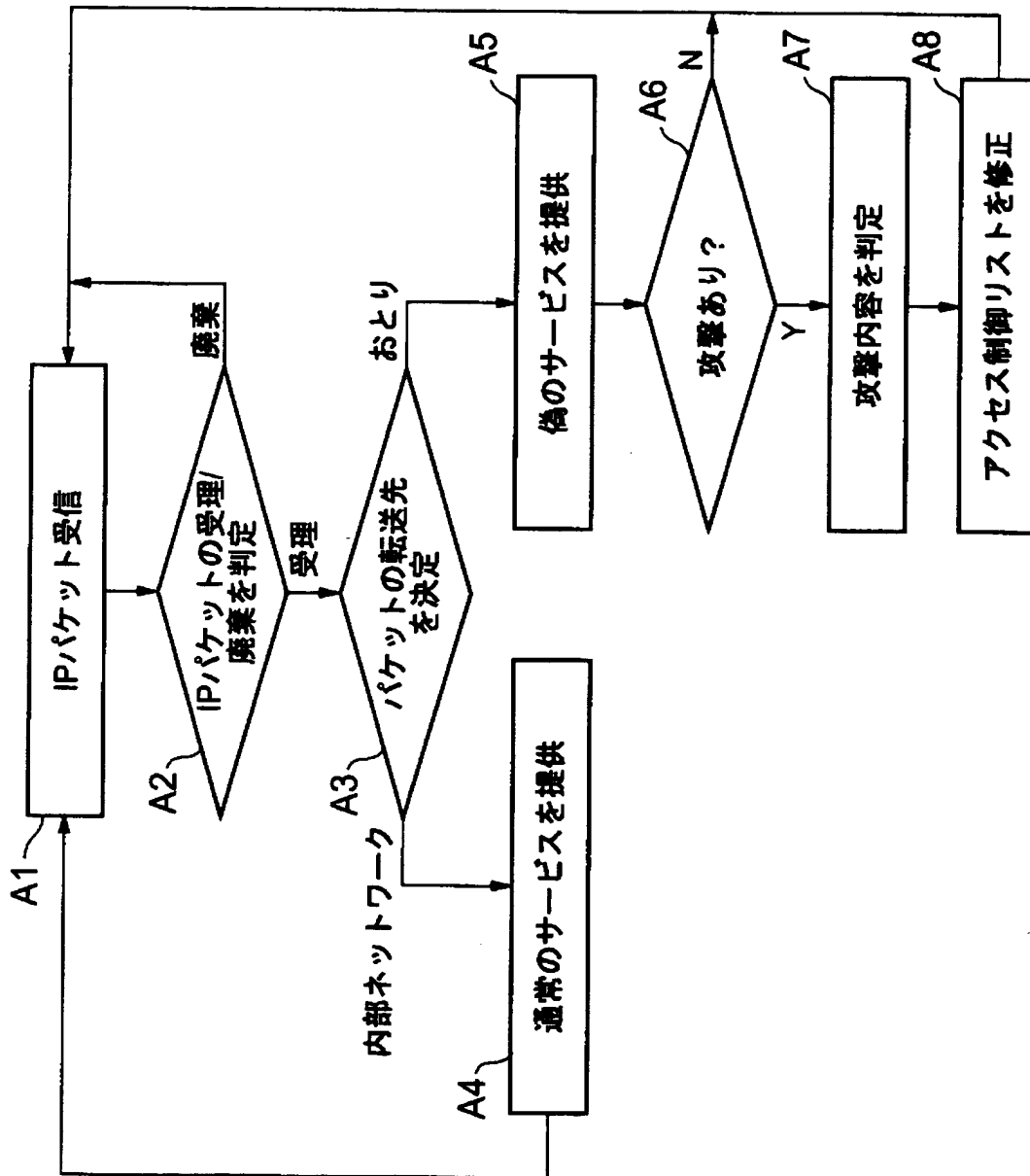
【図 6】

107 {

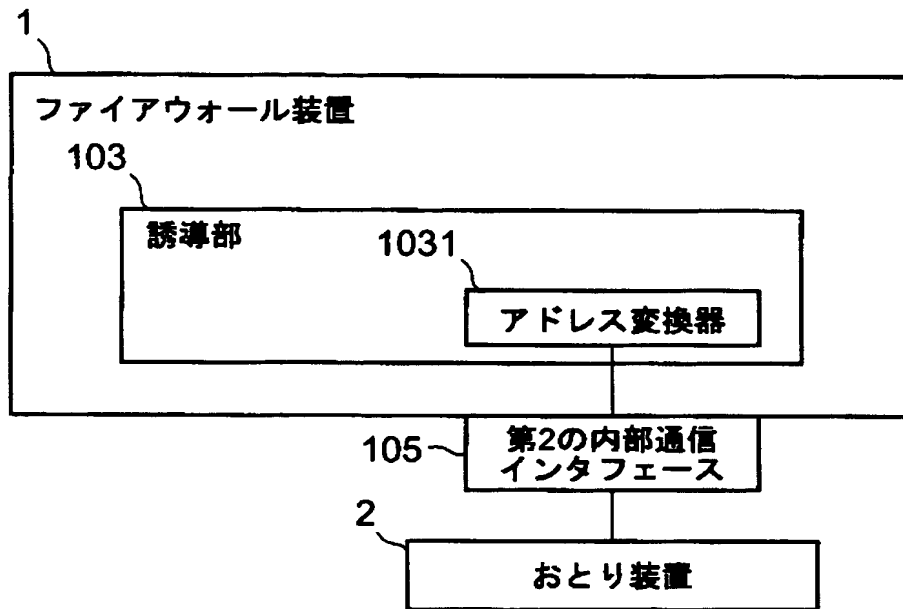
防御ルール判定部				
攻撃種別	ソースIPアドレス (SRC)	ディスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)	
RECON	—	—	—	
INTRUSION	\${SRC_IP_ADDRESS}	*	DROP	
DESTRUCTION	\${SRC_IP_ADDRESS}	*	DROP	

—…無指定(何もしない)
\${}…置換用変数

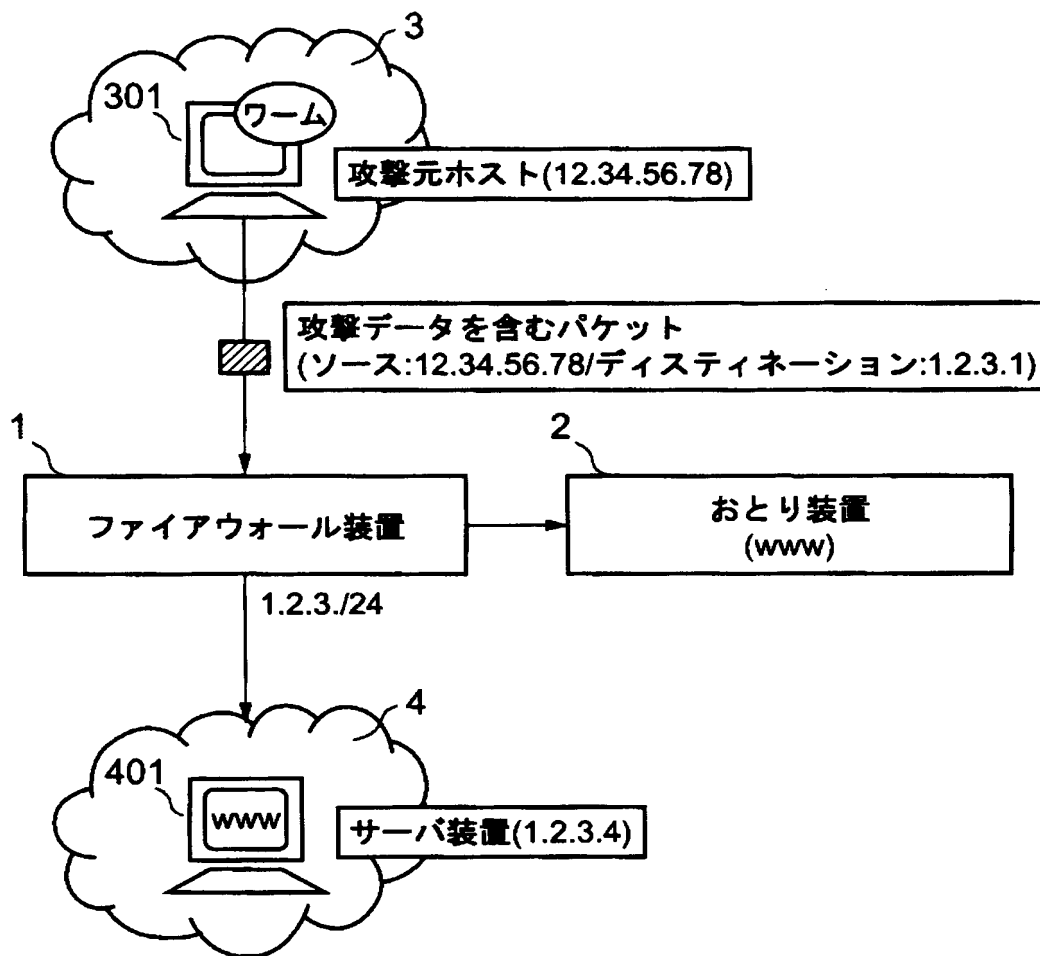
【図 7】



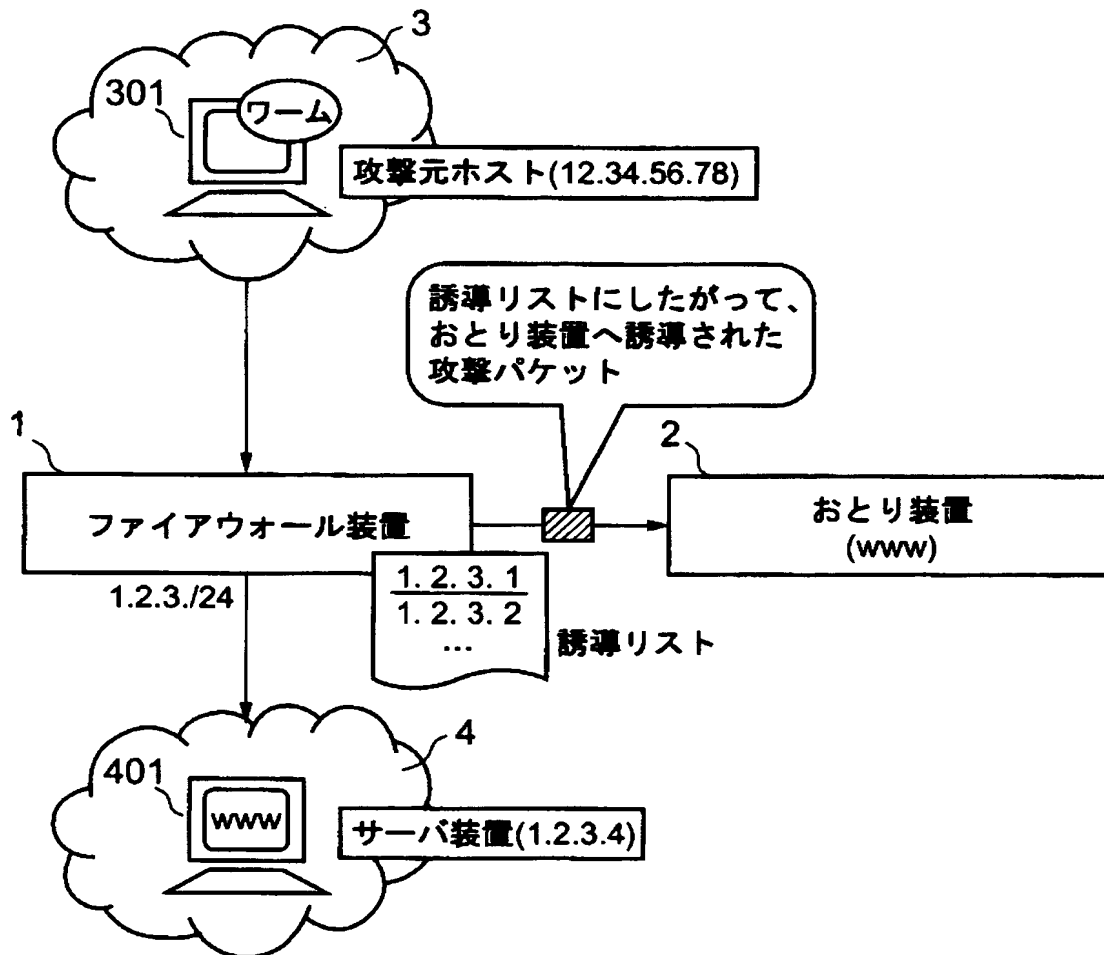
【図 8】



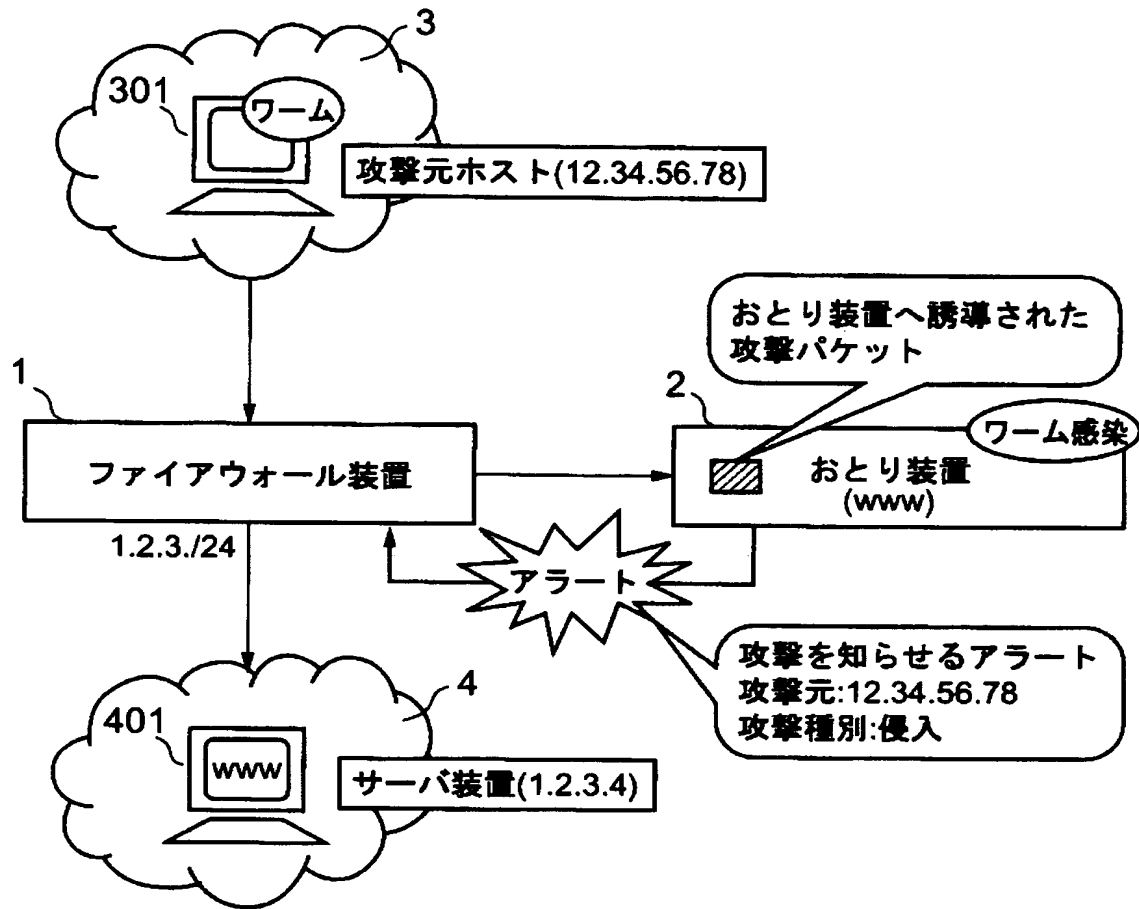
【図9】



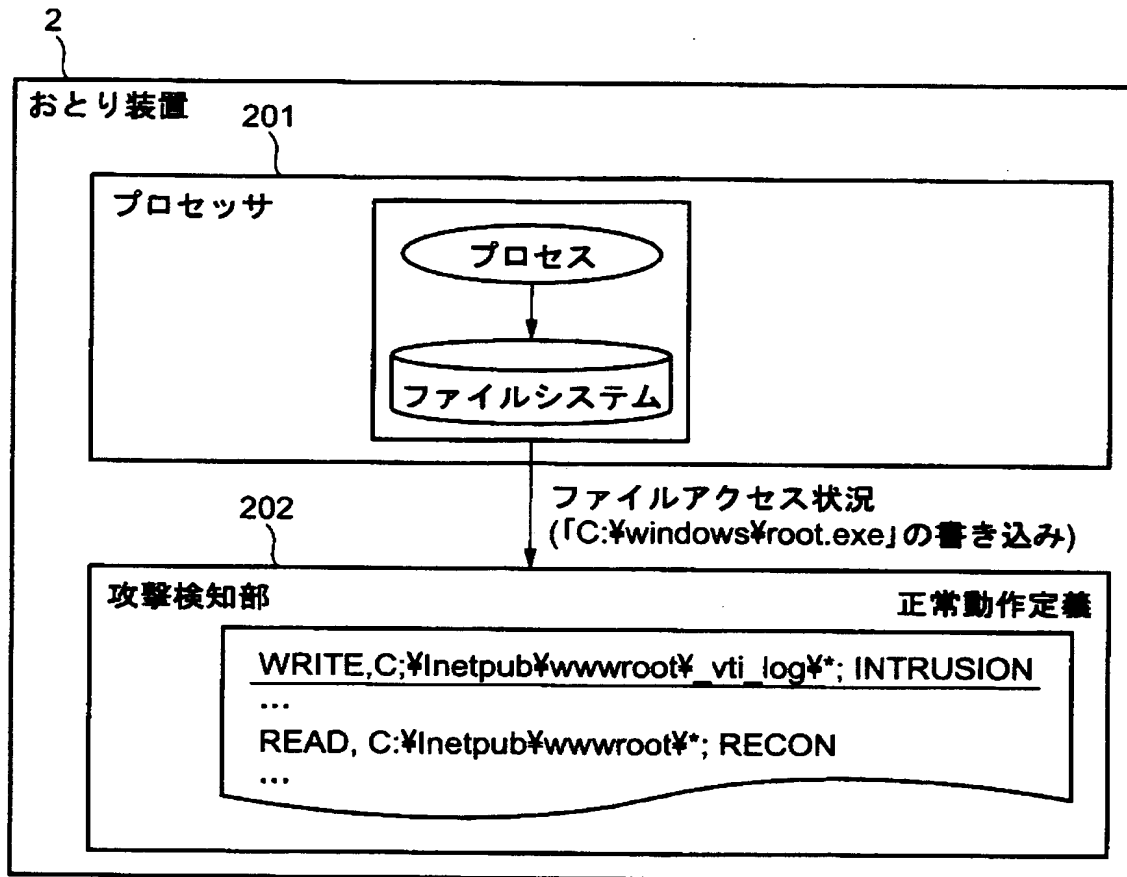
【図 10】



【図 11】



【図 12】



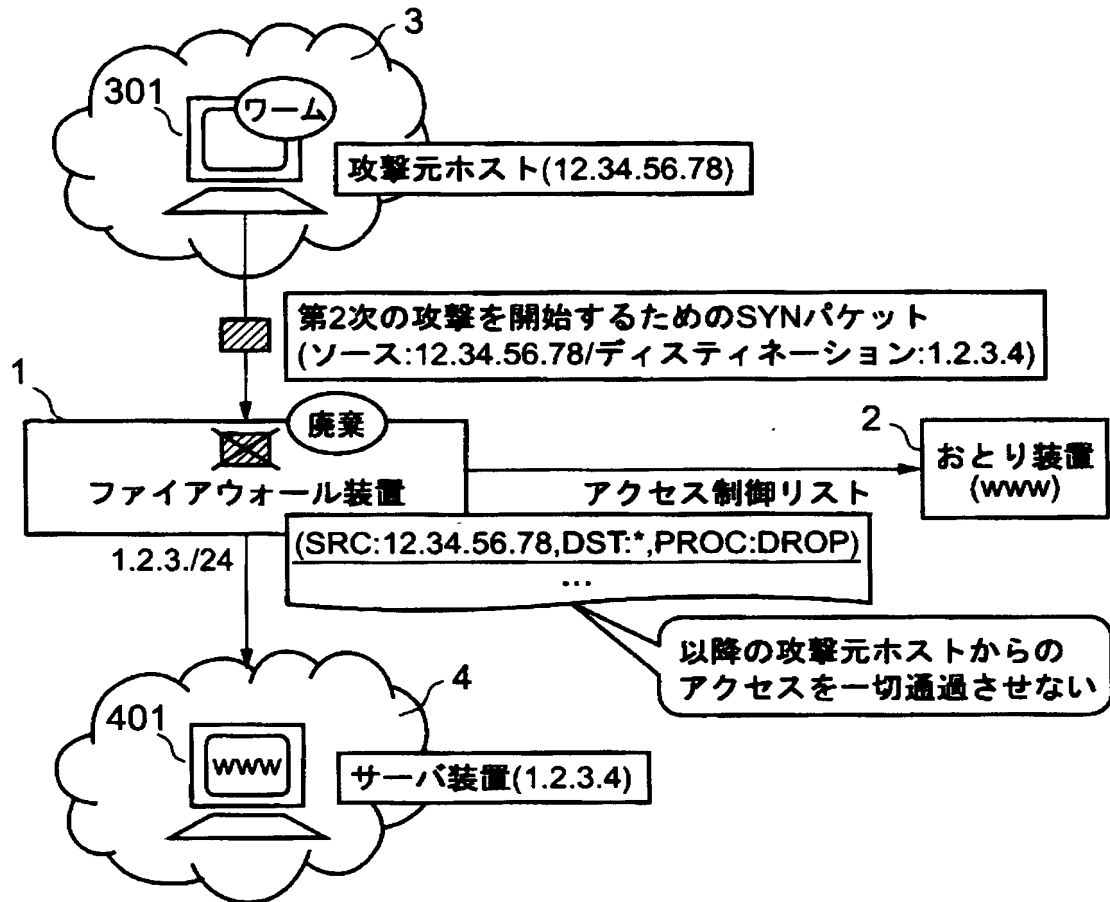
【図 1 3】

アクセス制御リストの更新

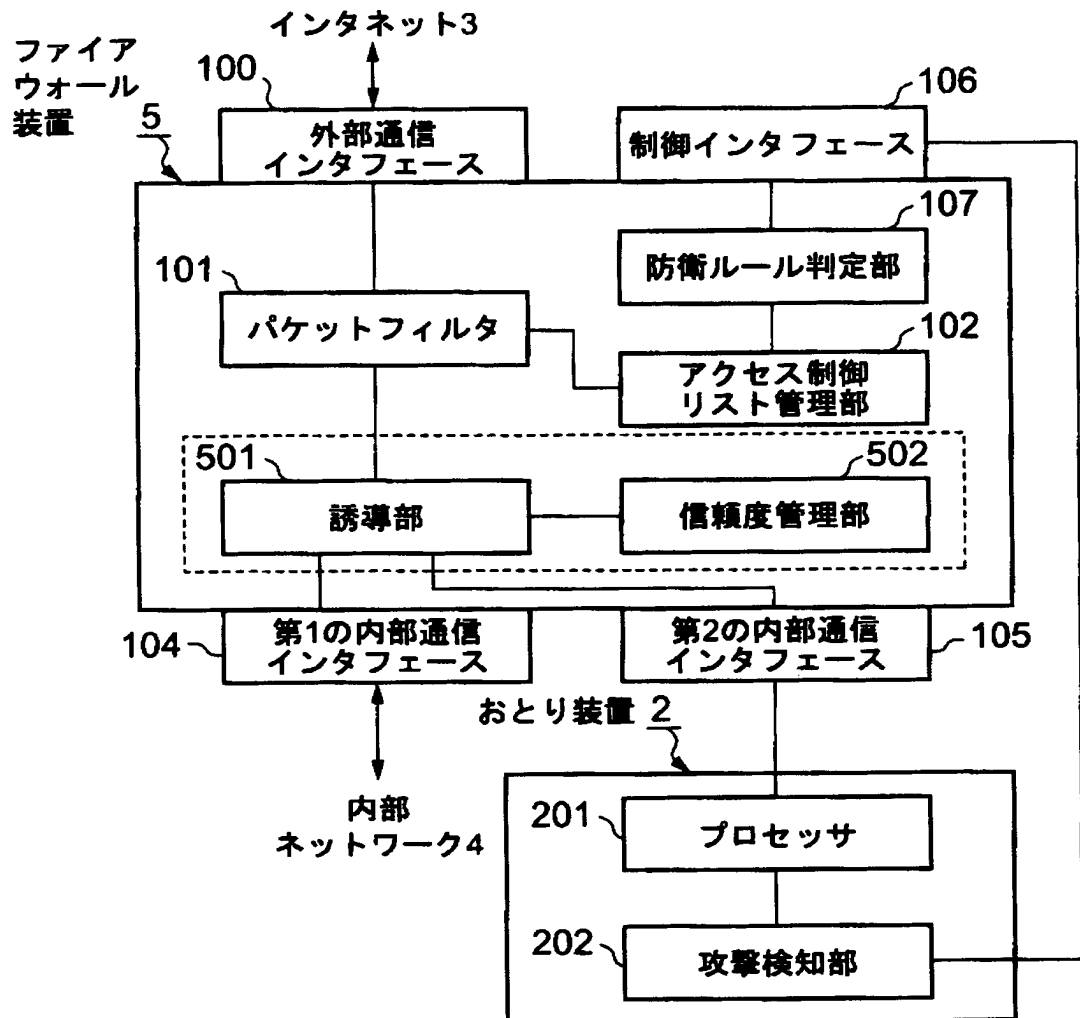
ソースIPアドレス (SRC)	デスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
12.34.56.78	*	DROP
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

追加

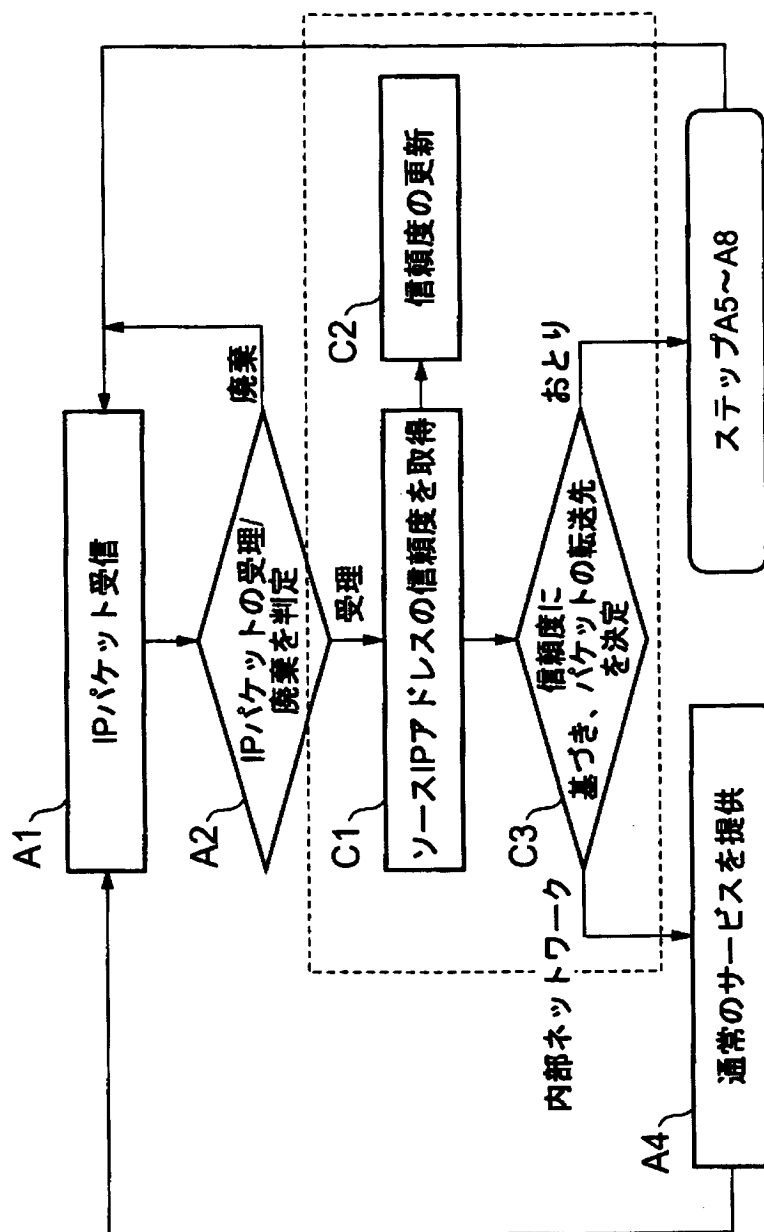
【図 14】



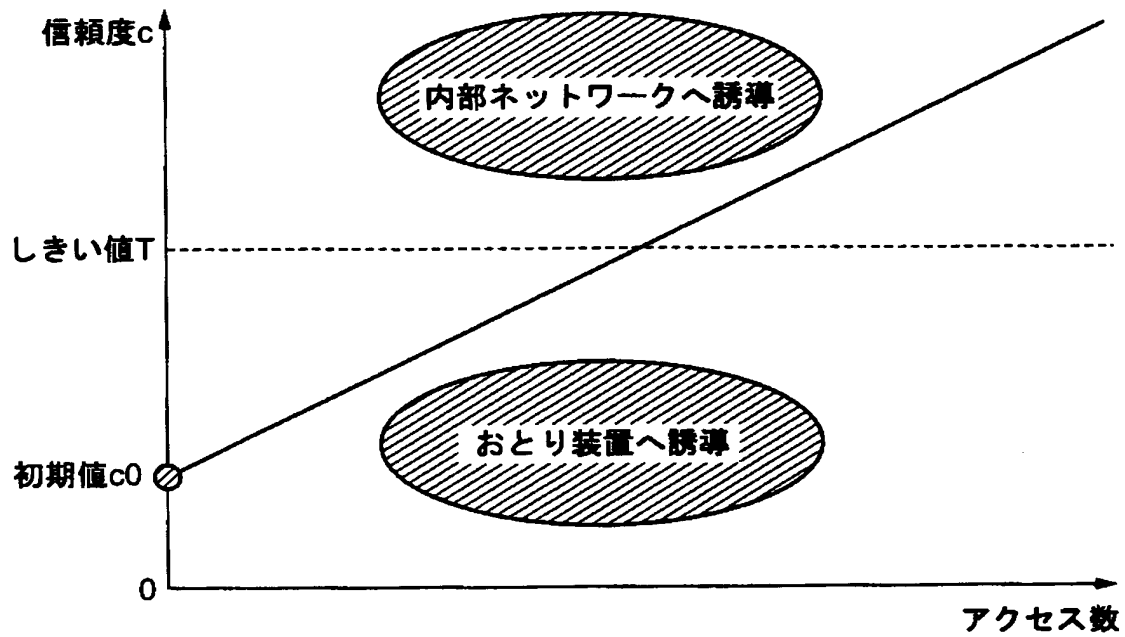
【図15】



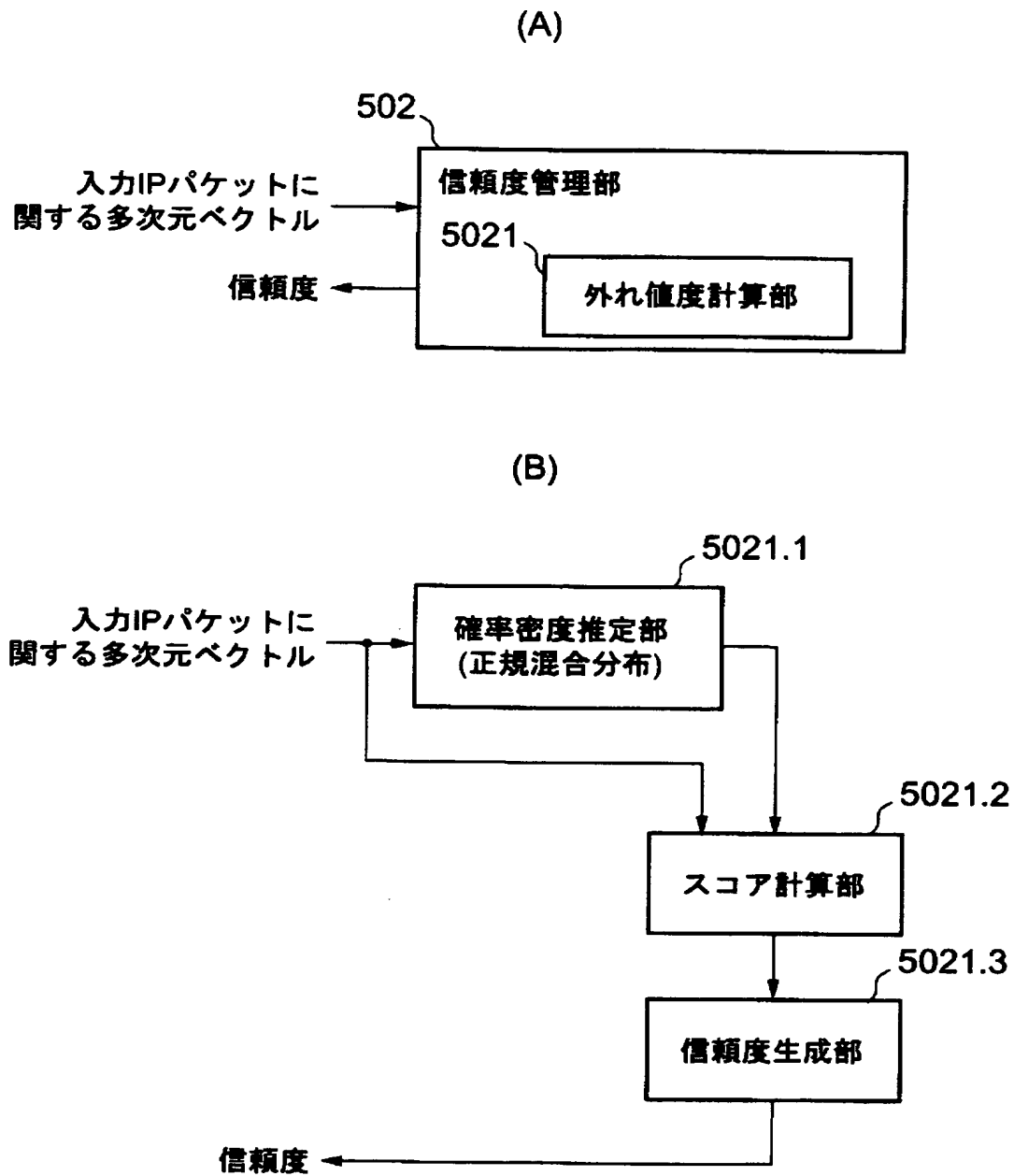
【図 16】



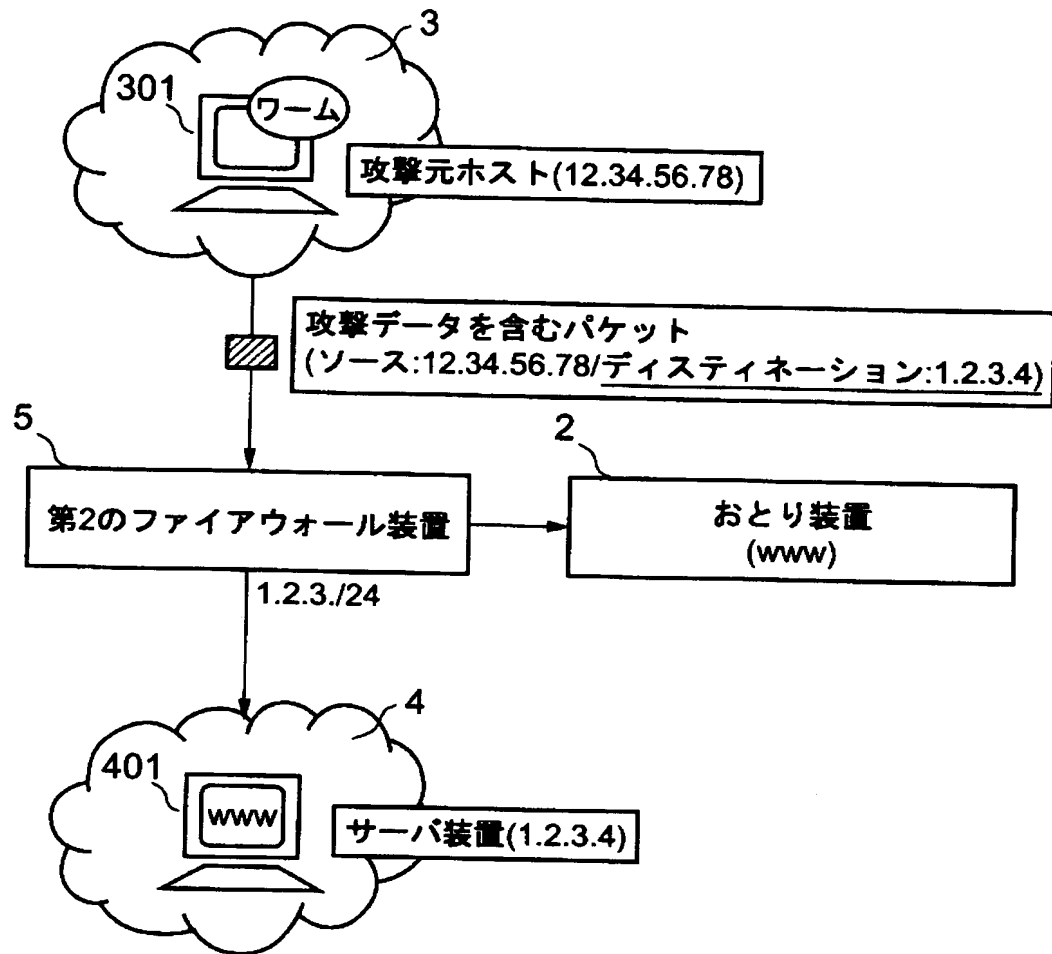
【図 17】



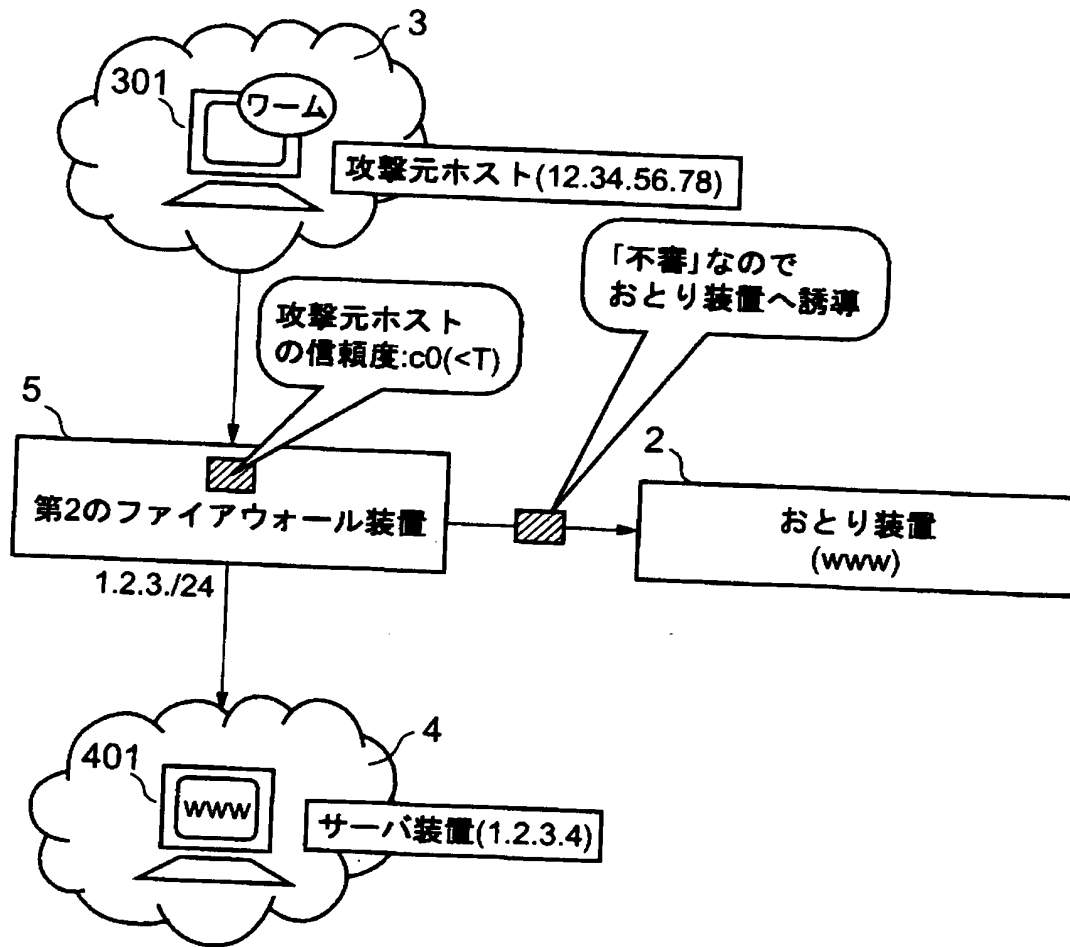
【図18】



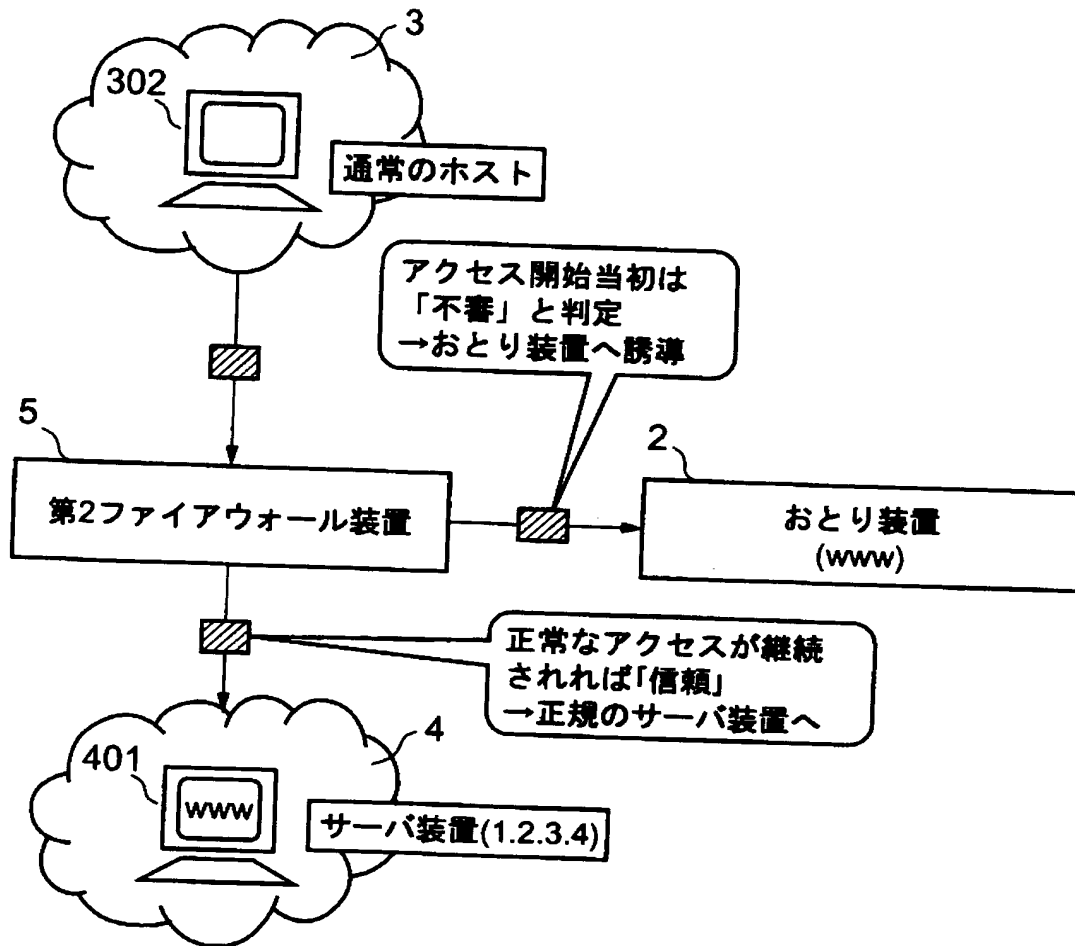
【図19】



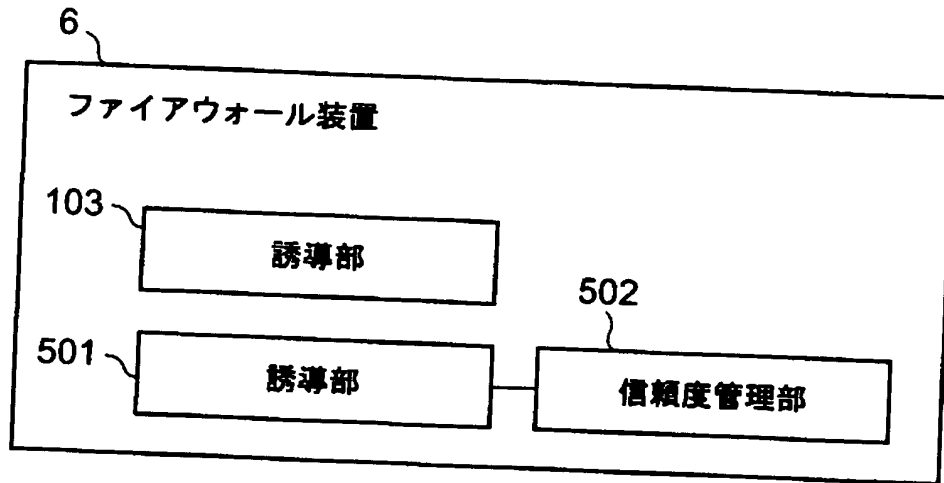
【図 20】



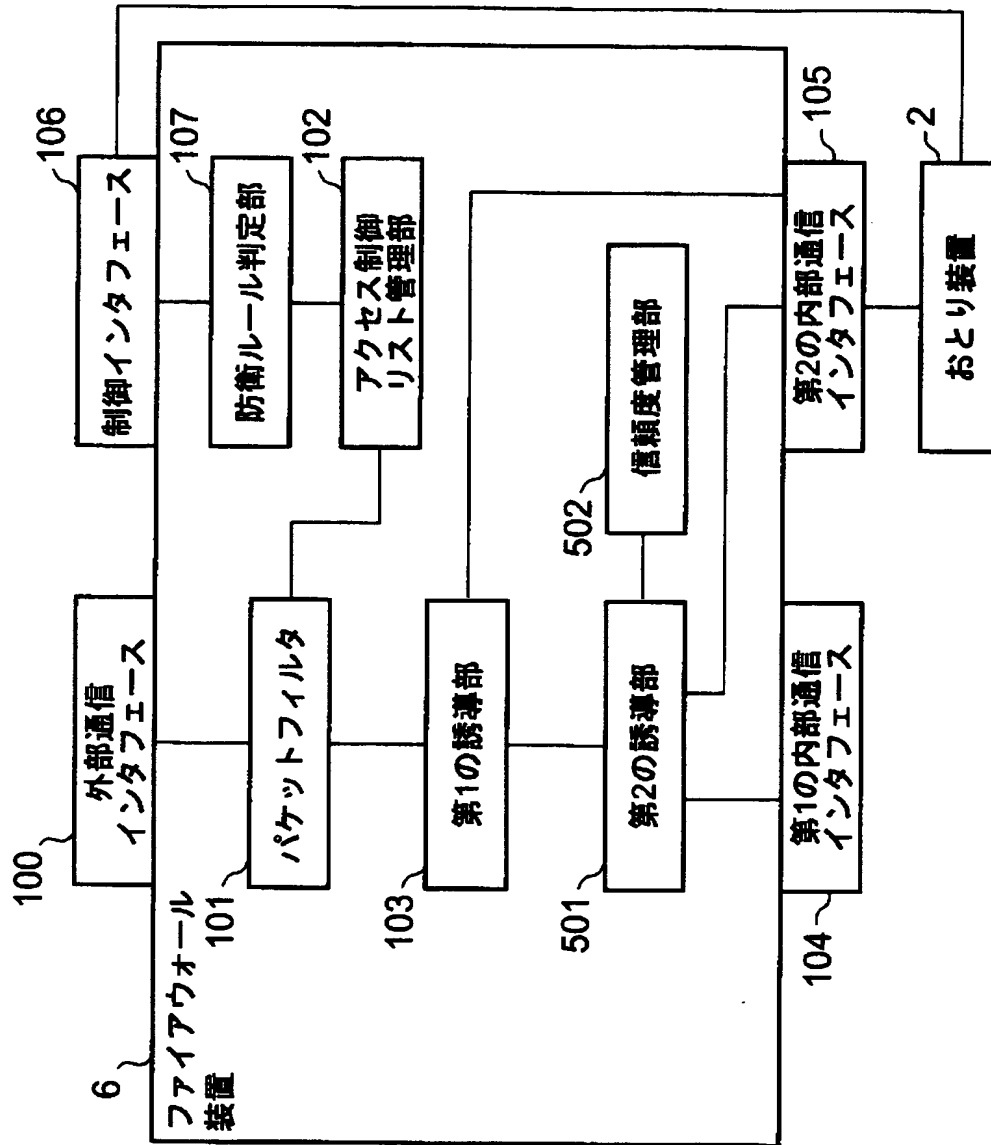
【図 21】



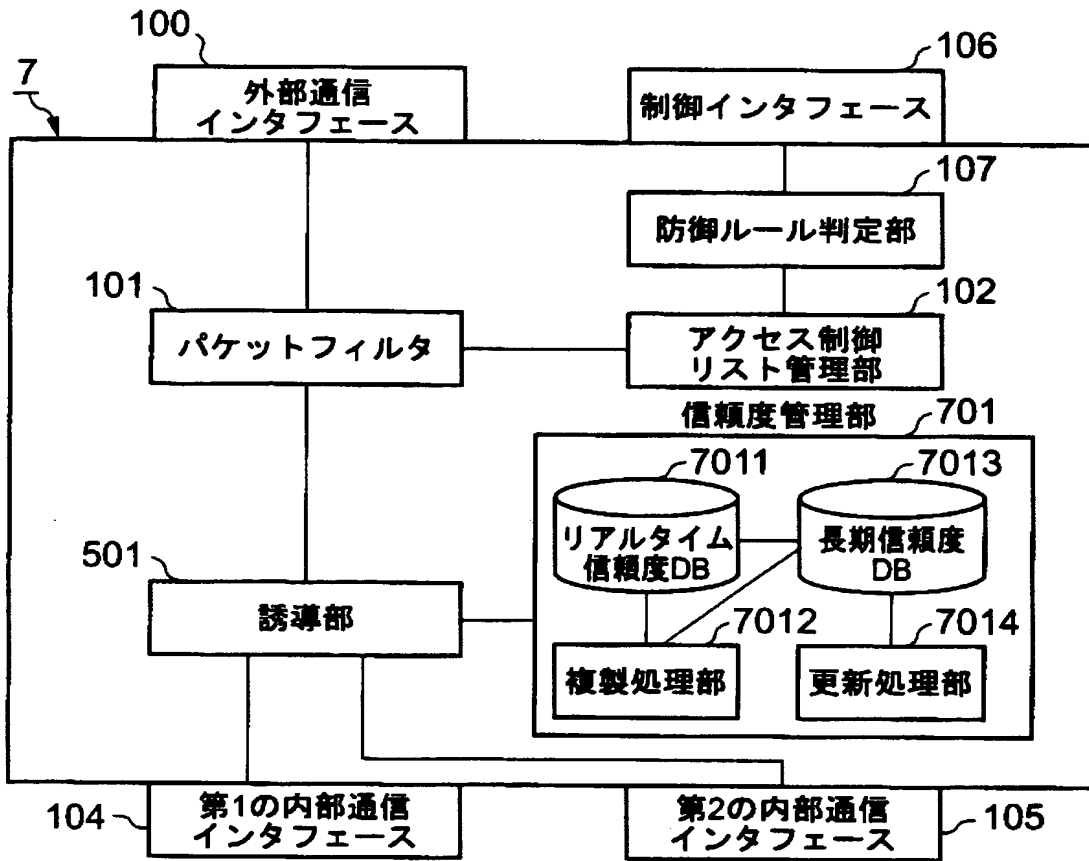
【図 22】



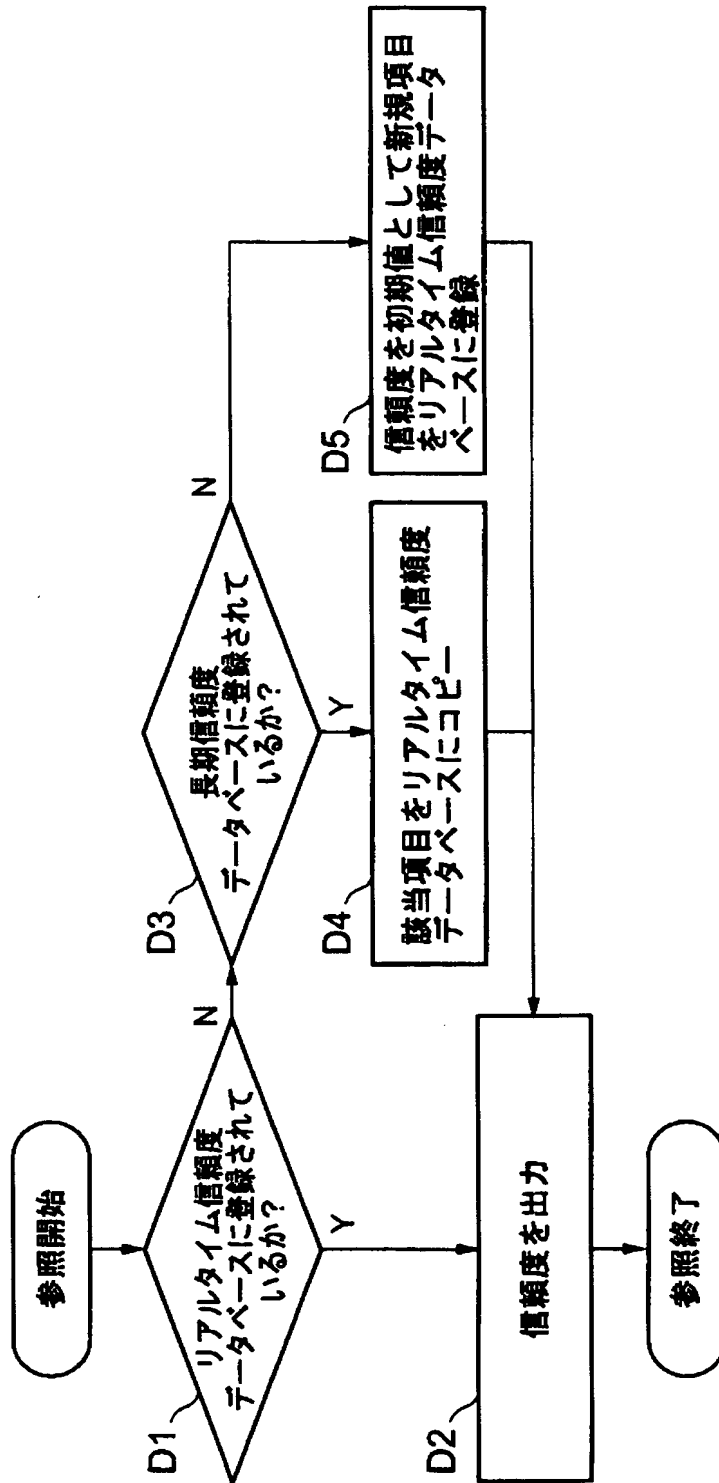
【図 2 3】



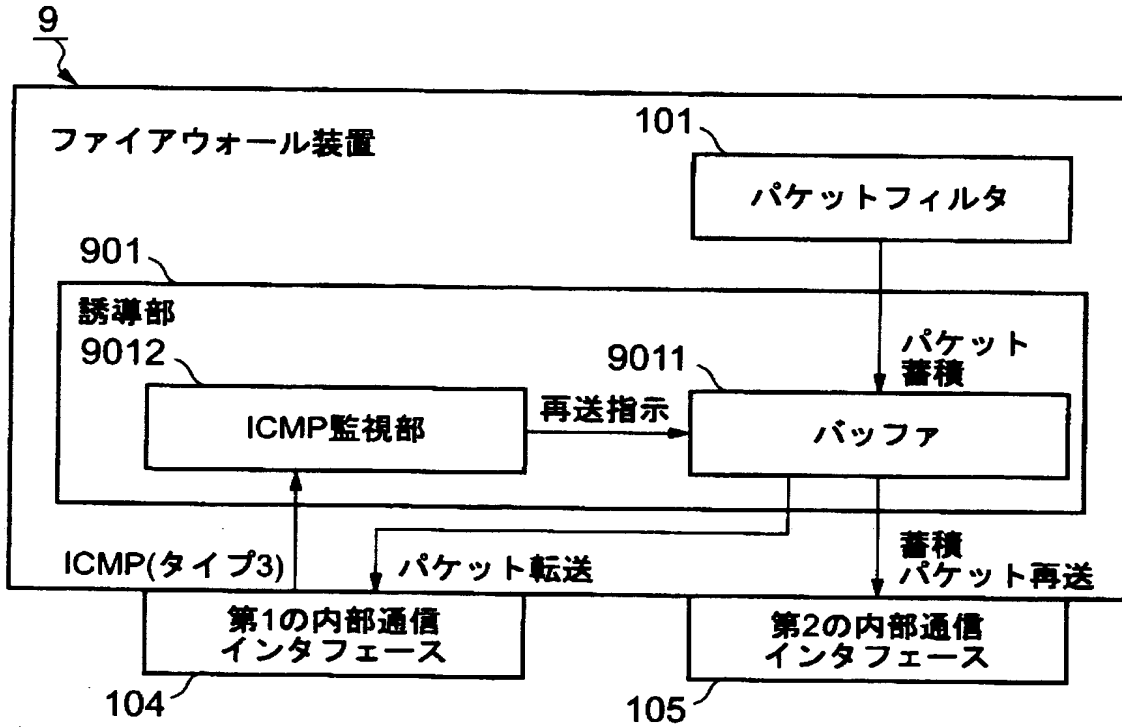
【図 24】



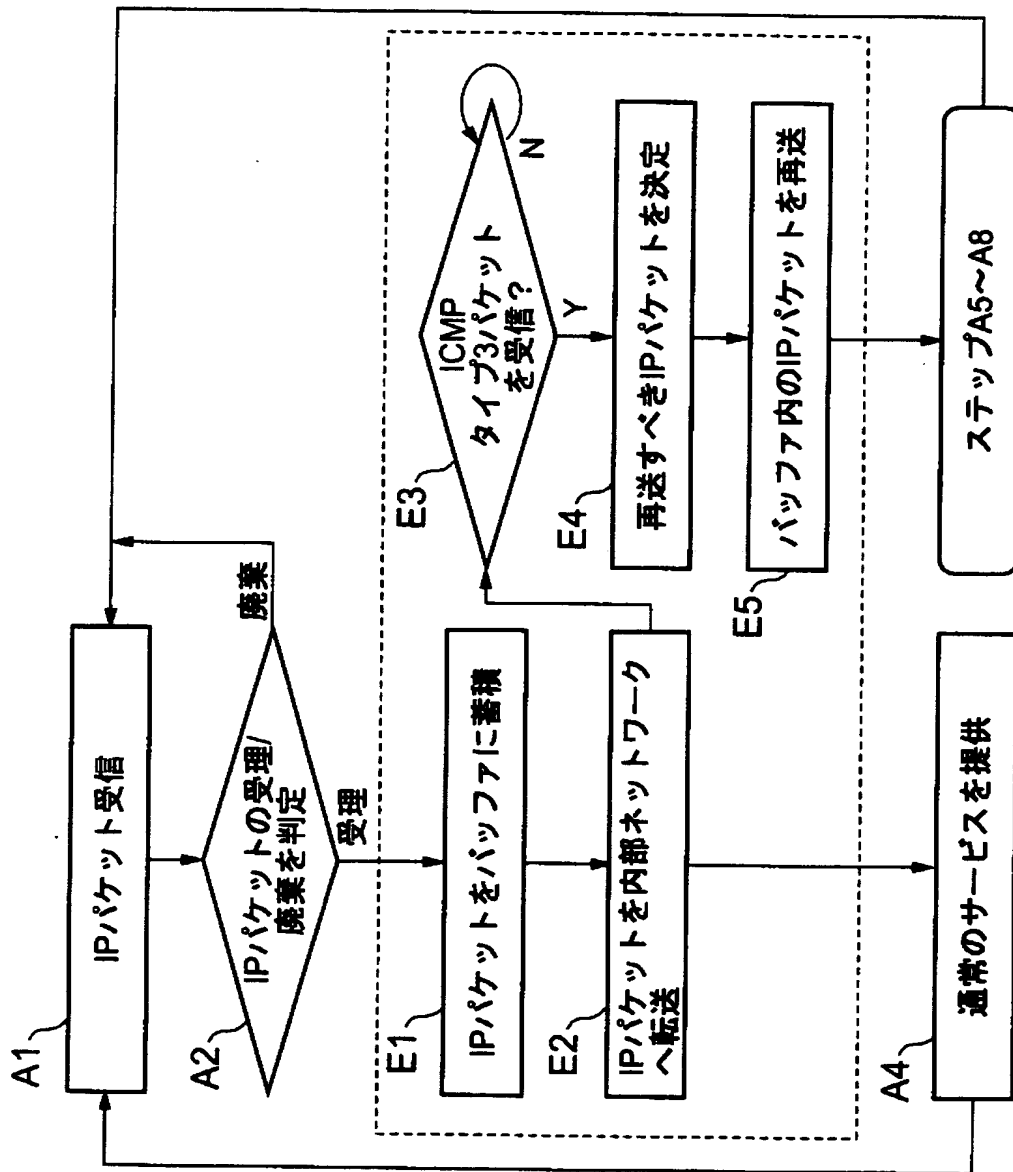
【図 25】



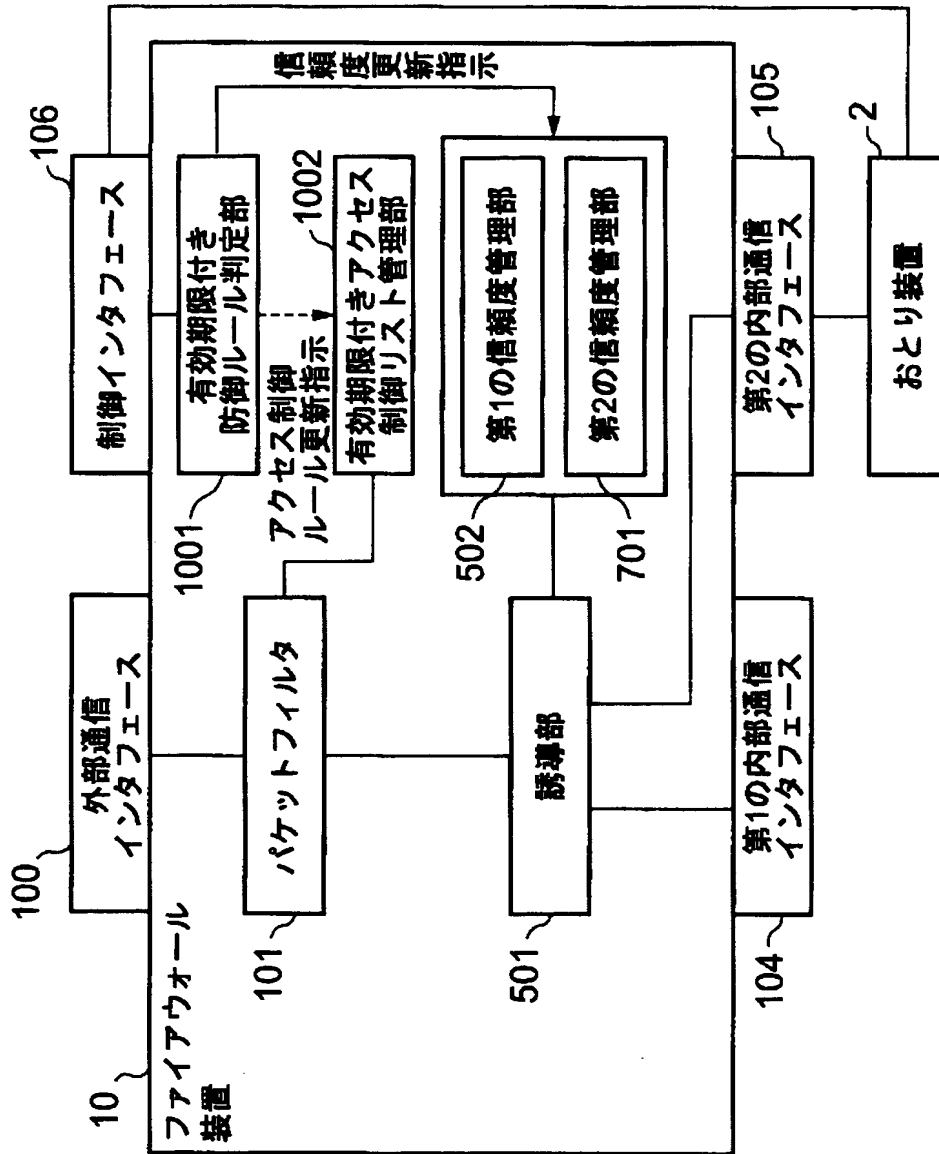
【図 26】



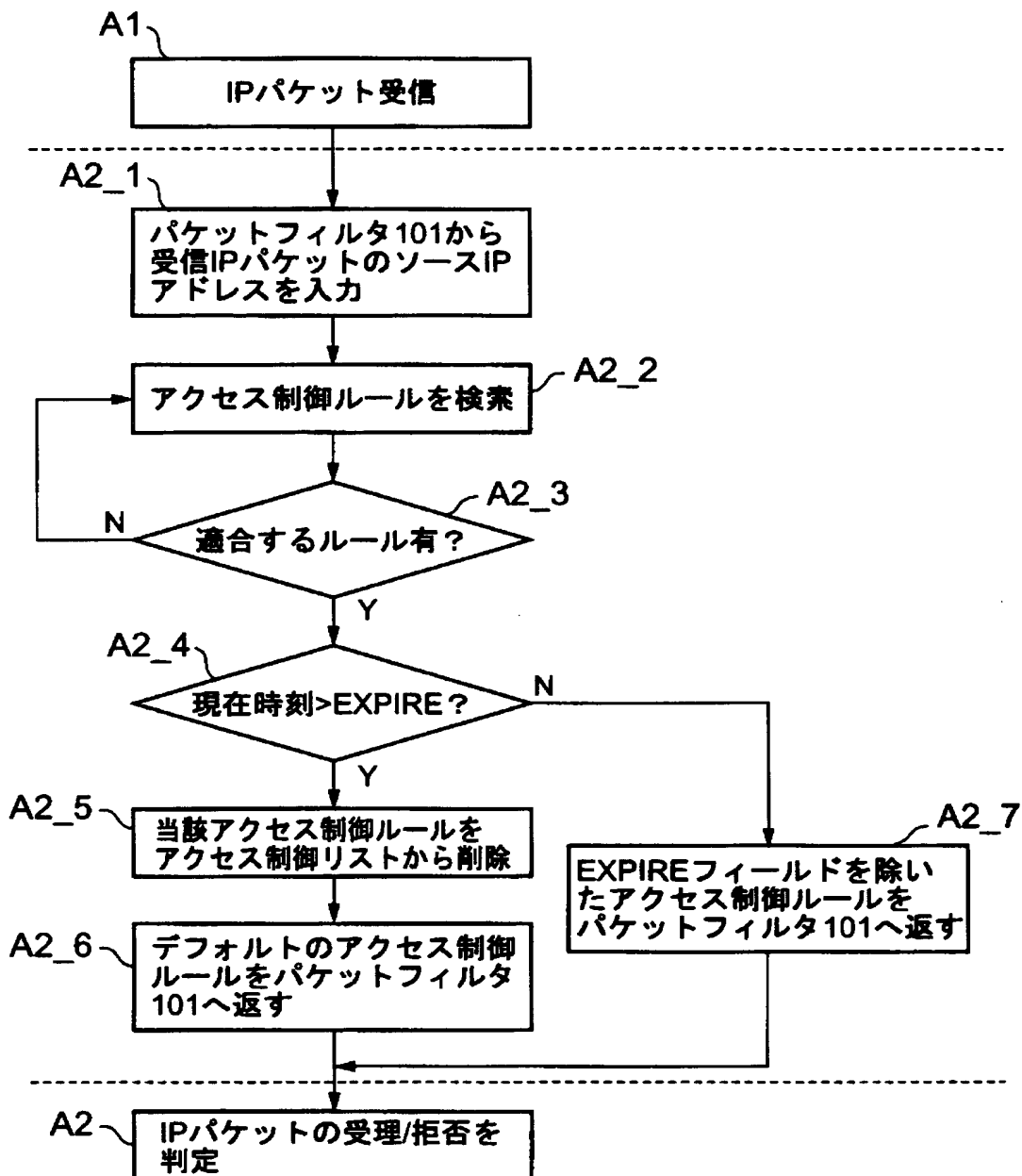
【図 27】



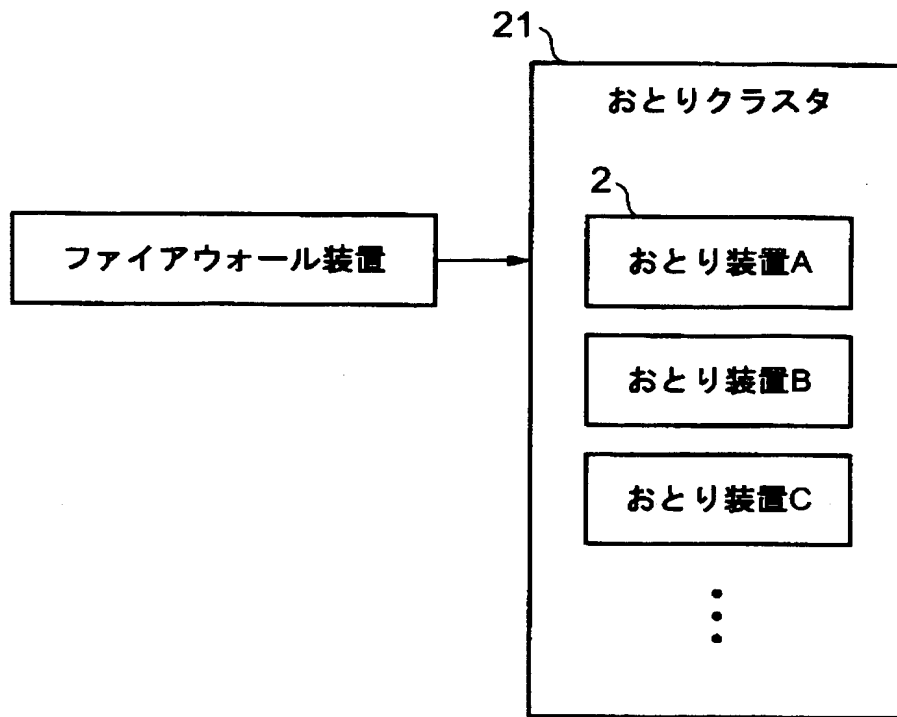
【図 28】



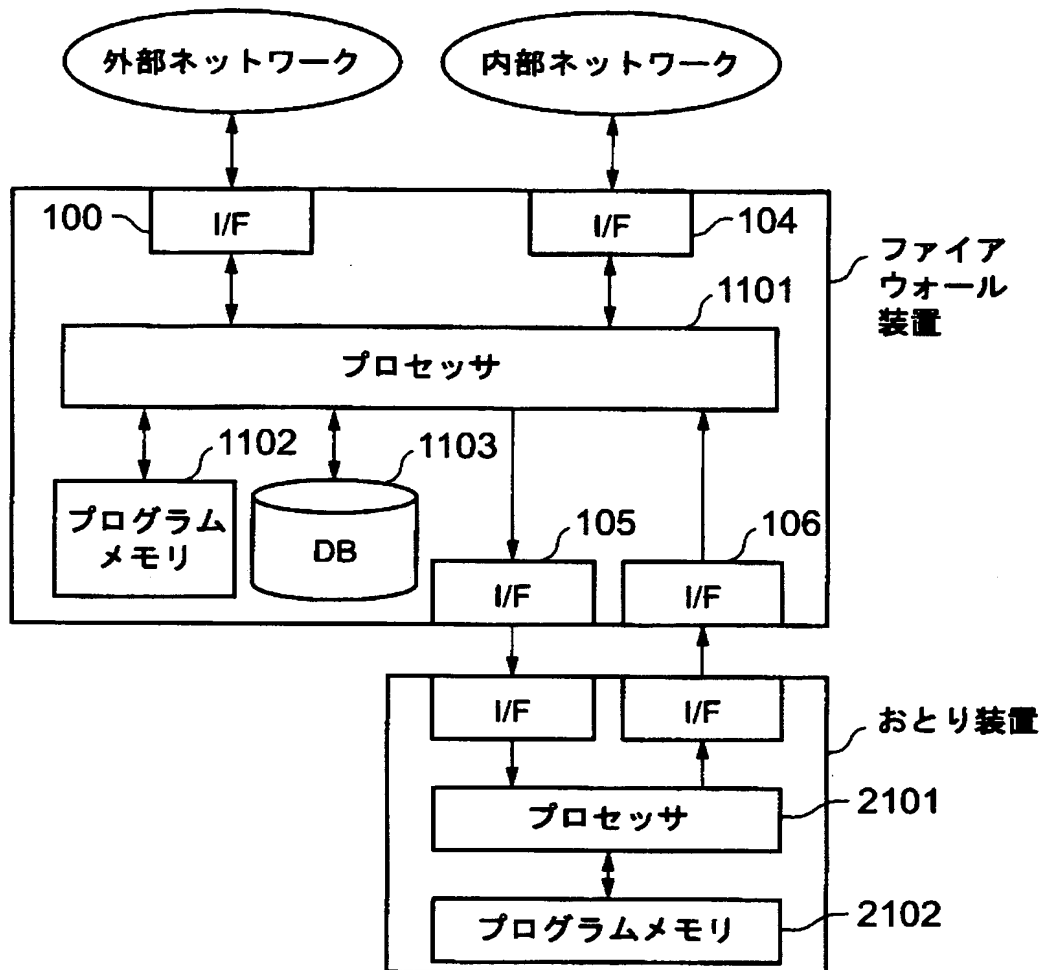
【図 29】



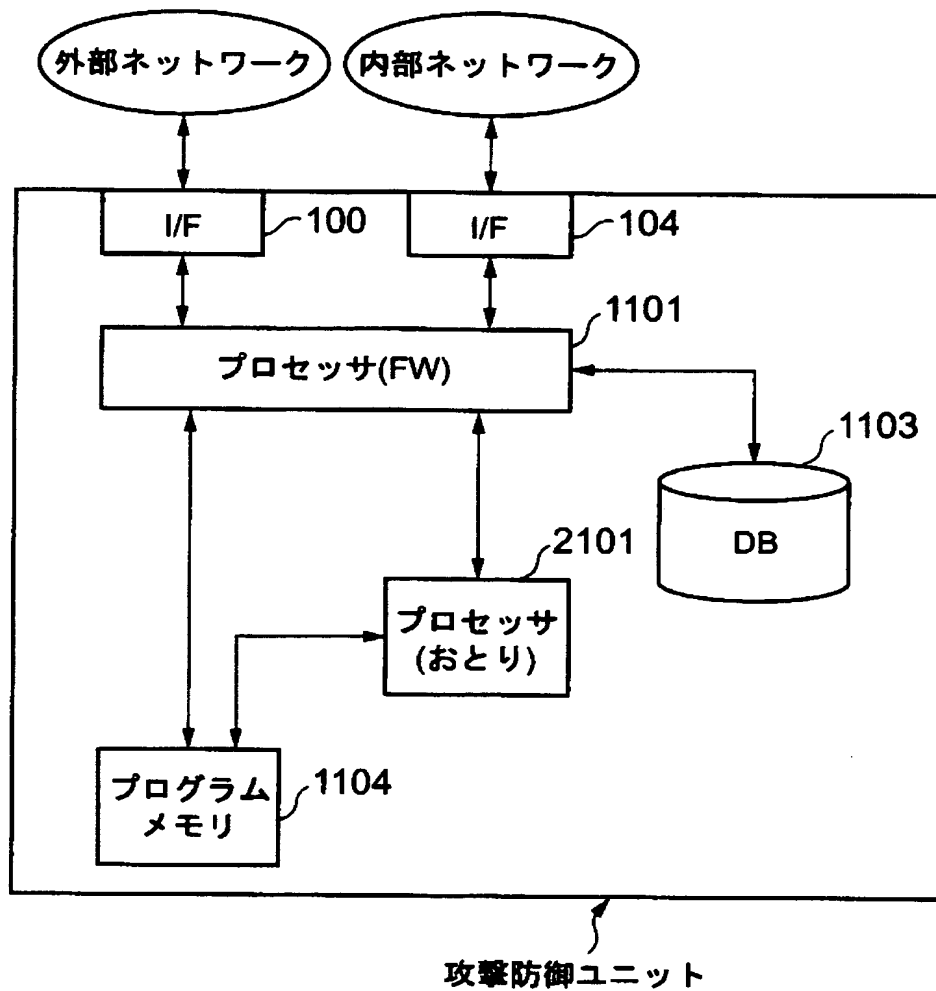
【図 30】



【図 31】



【図 32】



【書類名】 要約書

【要約】

【課題】 インターネットから内部ネットワークへのアクセスでSSLなど通信路暗号化技術が用いられた場合であっても不正なアクセスを検知し有効に防御する攻撃防御システム及び方法を提供する。

【解決部】 ファイアウォール装置1およびおとり装置2を備え、ファイアウォール装置1では、受け取ったIPパケットのヘッダ情報を参照し、所定のルールに基づいて攻撃の可能性がある「不審パケット」をおとり装置2へと誘導する。おとり装置2は、サービスを提供するプロセスを監視しながら、攻撃の有無を判定する。攻撃を検出した際には、攻撃元ホストのIPアドレスを含むアラートを生成してファイアウォール装置1に伝達する。当該アラートを受けたファイアウォール装置1は、以降、攻撃元ホストからのIPパケットの受入れを拒否する。

【選択図】 図2

特願 2 0 0 2 - 2 3 8 9 8 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社